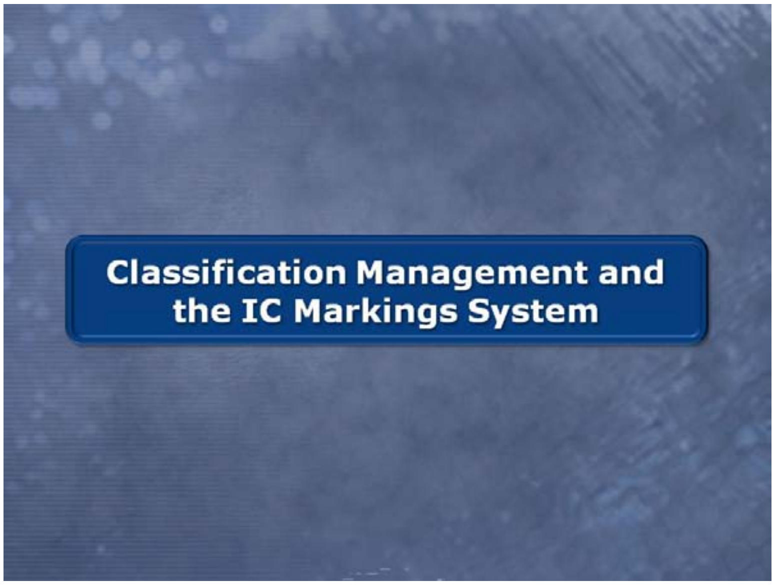
Classification Management and the Intelligence Community (IC) Markings System

Text Alternative

The Office of the Director of National Intelligence (ODNI)
Office of the National Counterintelligence Executive (ONCIX)

Last Updated: February 2012

Table of Contents



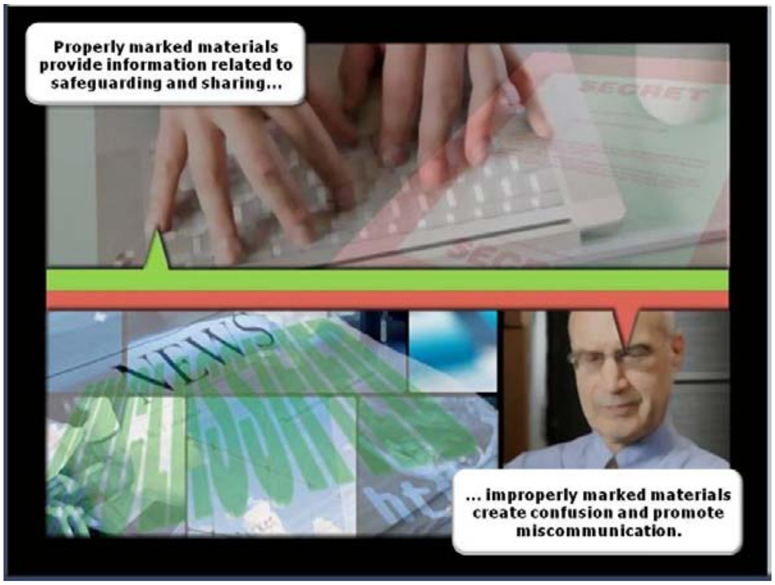
Classification Management and the IC Markings System

Classification Management and the IC Markings System

Classification decisions frequently have unforeseen impacts, the following narratives diverge from the point of one such decision, classified or unclassified?

Classification decisions frequently have unforeseen impacts, the following narratives diverge from the point of one such decision, classified or unclassified?

(Image alt: An authorized holder looking stern trying to make classification decisions that have unforeseen impacts. He questions whether or not if the document is classified or unclassified.)


Properly marked materials provide information related to safeguarding and sharing...
SECRET
NEWS
... improperly marked materials create confusion and promote miscommunication.

Properly marked materials provide information related to safeguarding and sharing…

… improperly marked materials create confusion and promote miscommunication.

(Image alt: Collage illustrating how properly marked materials provide information that is safeguarded versus improperly marked materials and how it can create confusion and miscommunication.)

Analysts create products from multiple sources in order to aid operational requirements and must apply markings to communicate protection of the information.
Mismarked information can lead to serious gaps in operations security practices that can be exploited by our adversaries.

Analysts create products from multiple sources in order to aid operational requirements and must apply marking to communicate protection of the information.

Mismarked information can lead to serious gaps in operations security practices that can be exploited by our adversaries.

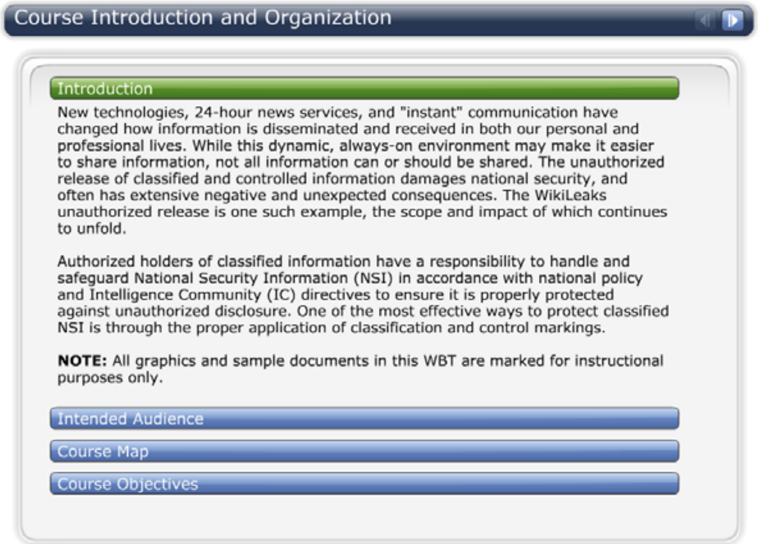
(Image alt: Collage illustrating how properly and improperly materials can have a major effect on operation security practices. A man and soldiers analyzing operational requirements to properly apply markings to communicate protection of information. Image of mismarked information and how it can be exploited by the adversary.)

Proper safeguarding and sharing creates positive outcomes and protects our national assets.

Improperly protected information can damage national security and harm those that depend on that vital information.

(Image alt: Collage illustrating the comparison of a solider with classified military equipment: missiles, bombs that has been properly safeguarded and the national assets are protected versus information being improperly protected damaging national security and harming others through exploding trucks, people and various infrastructure.)

(Image alt: Images illustrating that when information is properly marked a solider can come home safe and hug his mother versus information being improperly marked which can lead to potential death of soldiers and innocent people.)



New technologies, 24-hour news services, and "instant" communication have changed how information is disseminated and received in both our personal and professional lives. While this dynamic, always-on environment may make it easier to share information, not all information can or should be shared. The unauthorized release of classified and controlled information damages national security, and often has extensive negative and unexpected consequences. The WikiLeaks unauthorized release is one such example, the scope and impact of which continues to unfold.

Authorized holders of classified information have a responsibility to handle and safeguard National Security Information (NSI) in accordance with national policy and Intelligence Community (IC) directives to ensure it is properly protected against unauthorized disclosure. One of the most effective ways to protect classified NSI is through the proper application of classification and control markings.

NOTE: All graphics and sample documents in this WBT are marked for instructional purposes only.

Course Introduction and Organization

Introduction

New technologies, 24-hour news services, and "instant" communication have changed how information is disseminated and received in both our personal and professional lives. While this dynamic, always-on environment may make it easier to share information, not all information can or should be shared. The unauthorized release of classified and controlled information damages national security, and often has extensive negative and unexpected consequences. The WikiLeaks unauthorized release is one such example, the scope and impact of which continues to unfold.

Authorized holders of classified information have a responsibility to handle and safeguard National Security Information (NSI) in accordance with national policy and Intelligence Community (IC) directives to ensure it is properly protected against unauthorized disclosure. One of the most effective ways to protect classified NSI is through the proper application of classification and control markings.

NOTE: All graphics and sample documents in this WBT are marked for instructional purposes only.

Intended Audience

The *Classification Management and the IC Markings System* course is intended to train IC element personnel, providing a complete and common understanding of the classification and control markings system (as directed by the Intelligence Community Directive (ICD) 710). This course also meets the minimum national training requirements for derivative classifiers established in Executive Order (EO) 13526 and the Information Security Oversight Office (ISOO) Implementing Directive.

This training may also be beneficial to the following Non-National Intelligence Program (Non-NIP) elements:

- The Executive Office of the President
- The United States (US) Legislative and Judicial Branches
- State, local, tribal, and private sector (SLTP) entities
- Non-Title 50 organizations
- Private sector organizations

Course Map

The *Classification Management and the IC Markings System* course consists of four lessons which are further broken down into topics. The course should be taken in succession as each topic builds on the next; however, the course also may be used as a reference tool and browsed by topic. This training is unclassified in its entirety.

(Image alt: Course map showing lessons and topics)

Course Objectives

Lesson 1: *History and Background of Classification Management*

- Describe National Security Information (NSI)
- Describe why information is classified
- Describe the IC classification and control markings system

- Describe the requirements for authorized access to classified NSI

Lesson 2: *Classification and Control Markings Principles*

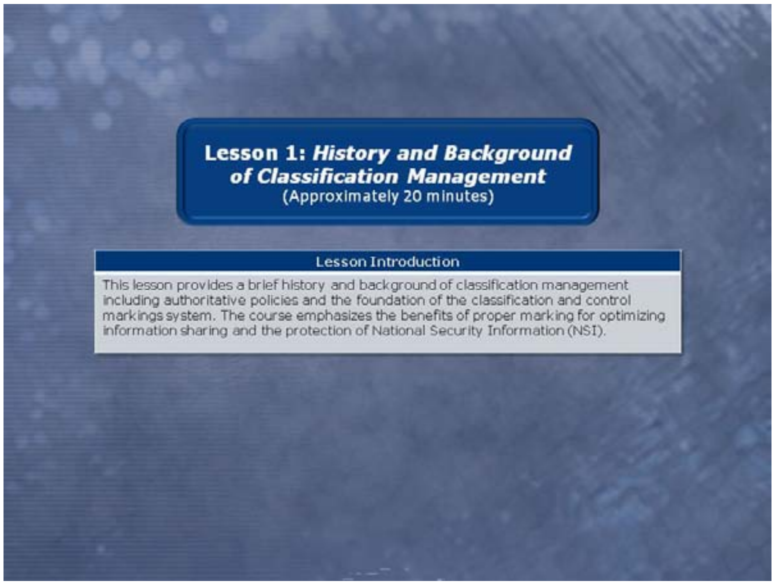
- Distinguish between the two types of classification authorities
- Discriminate between classified and unclassified information
- Describe the required marking elements of classified and unclassified NSI
- Identify classification marking guidance available to derivative classifiers

Lesson 3: *The IC Markings System - Beyond Basic Principles*

- Identify and describe the nine categories of markings
- Apply classification and control markings in accordance with the *Controlled Access Program Coordination Office (CAPCO) Register and Manual*

Lesson 4: The *IC Markings System - Practical Application of Markings*

- Illustrate appropriate application and sequencing of classification and control markings in NSI
- Apply markings consistent with established marking, commingling, and precedence rules



Lesson 1: *History and Background of Classification Management*
(Approximately 20 minutes)

Lesson Introduction

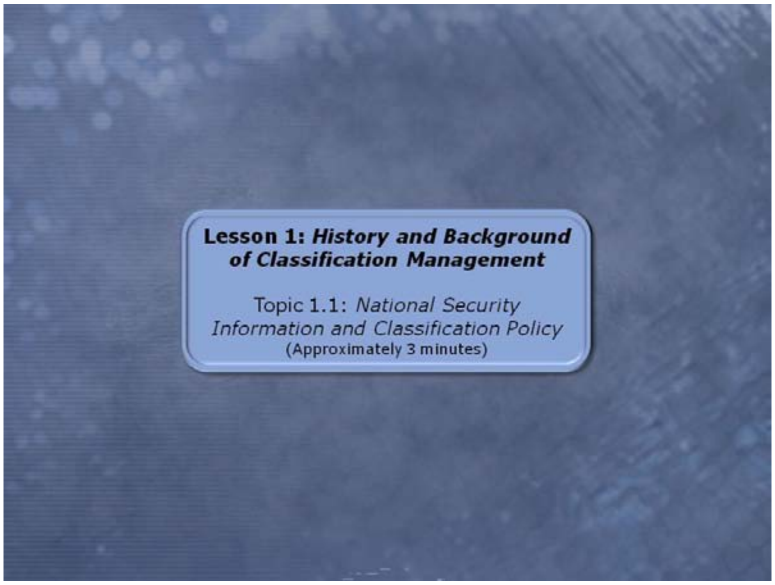
This lesson provides a brief history and background of classification management including authoritative policies and the foundation of the classification and control markings system. The course emphasizes the benefits of proper marking for optimizing information sharing and the protection of National Security Information (NSI).

Lesson 1: *History and Background of Classification Management*

(Approximately 20 minutes)

Lesson Introduction

This lesson provides a brief history and background of classification management including authoritative policies and the foundation of the classification and control markings system. The course emphasizes the benefits of proper marking for optimizing information sharing and the protection of National Security Information (NSI).



Lesson 1: ***History and Background of Classification Management***

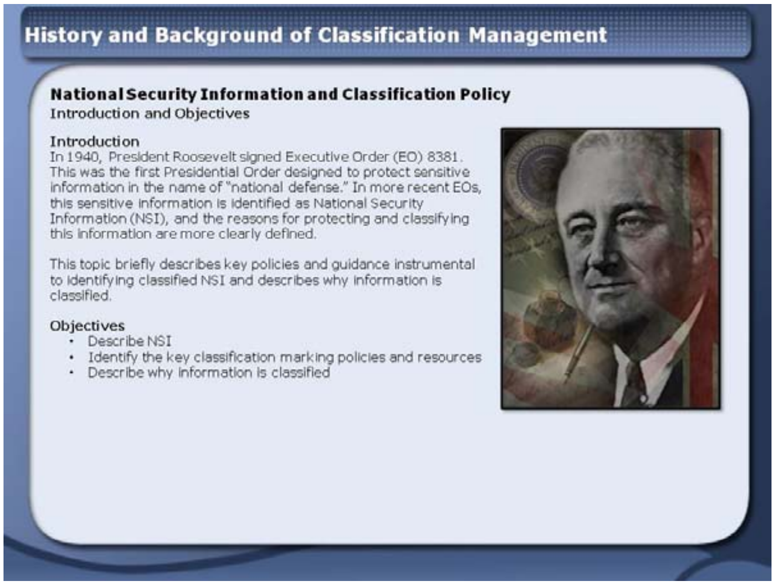
Topic 1.1: *National Security Information and Classification Policy*

(Approximately 3 minutes)

Lesson 1: *History and Background of Classification Management*

Topic 1.1: *National Security Information and Classification Policy*

(Approximately 3 minutes)



History and Background of Classification Management

National Security Information and Classification Policy

Introduction and Objectives

Introduction

In 1940, President Roosevelt signed Executive Order (EO) 8381. This was the first Presidential Order designed to protect sensitive information in the name of "national defense." In more recent EOs, this sensitive information is identified as National Security Information (NSI), and the reasons for protecting and classifying this information are more clearly defined.

This topic briefly describes key policies and guidance instrumental to identifying classified NSI and describes why information is classified.

Objectives

- Describe NSI
- Identify the key classification marking policies and resources
- Describe why information is classified

Introduction and Objectives

Introduction

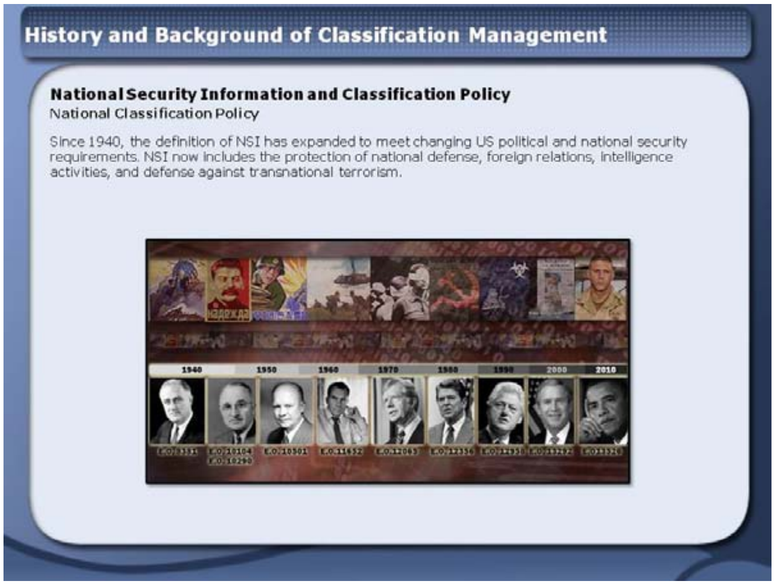
In 1940, President Roosevelt signed Executive Order (EO) 8381. This was the first Presidential Order designed to protect sensitive information in the name of "national defense." In more recent EOs, this sensitive information is identified as National Security Information (NSI), and the reasons for protecting and classifying this information are more clearly defined.

This topic briefly describes key policies and guidance instrumental to identifying classified NSI and describes why information is classified.

Objectives

- Describe NSI
- Identify the key classification marking policies and resources
- Describe why information is classified

(Image alt: President Roosevelt in front of a collage of the signed EO 8381 to protect sensitive information, pen, ink, US flag, and President of the US emblem.)



History and Background of Classification Management

National Security Information and Classification Policy

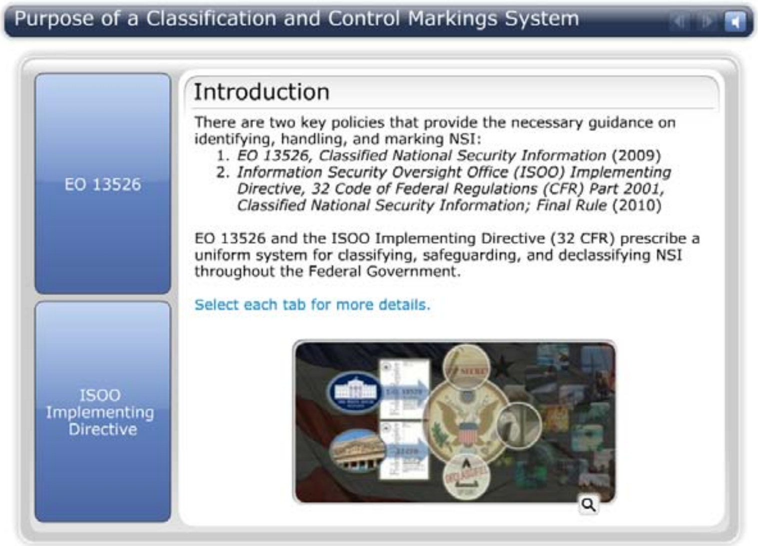
National Classification Policy

Since 1940, the definition of NSI has expanded to meet changing US political and national security requirements. NSI now includes the protection of national defense, foreign relations, intelligence activities, and defense against transnational terrorism.

National Classification Policy

Since 1940, the definition of NSI has expanded to meet changing US political and national security requirements. NSI now includes the protection of national defense, foreign relations, intelligence activities, and defense against transnational terrorism.

(Image alt: Presidents from 1940 to 2010: Roosevelt, Truman, Eisenhower, Nixon, Carter, Regan, Clinton, Bush, and Obama in front of a collage of a soldier, Soviet Union flag, New York Times newspaper on 9/11 attack, people blind folded, and war.)


Purpose of a Classification and Control Markings System
EO 13526
ISOO Implementing Directive

Introduction

There are two key policies that provide the necessary guidance on identifying, handling, and marking NSI:

1. *EO 13526, Classified National Security Information* (2009)
2. *Information Security Oversight Office (ISOO) Implementing Directive, 32 Code of Federal Regulations (CFR) Part 2001, Classified National Security Information; Final Rule* (2010)

EO 13526 and the ISOO Implementing Directive (32 CFR) prescribe a uniform system for classifying, safeguarding, and declassifying NSI throughout the Federal Government.

Select each tab for more details.

Purpose of a Classification and Control Markings System

Introduction

There are two key policies that provide the necessary guidance on identifying, handling, and marking NSI:

1. *EO 13526, Classified National Security Information* (2009)
2. *Information Security Oversight Office (ISOO) Implementing Directive, 32 Code of Federal Regulations (CFR) Part 2001, Classified National Security Information; Final Rule* (2010)

EO 13526 and the ISOO Implementing Directive (32 CFR) prescribe a uniform system for classifying, safeguarding, and declassifying NSI throughout the Federal Government.

(Interaction alt: Interaction with overview information of two key policies including EO 13526 and ISOO Implementing Directive 32 CFR Part 2001.)

EO 13526

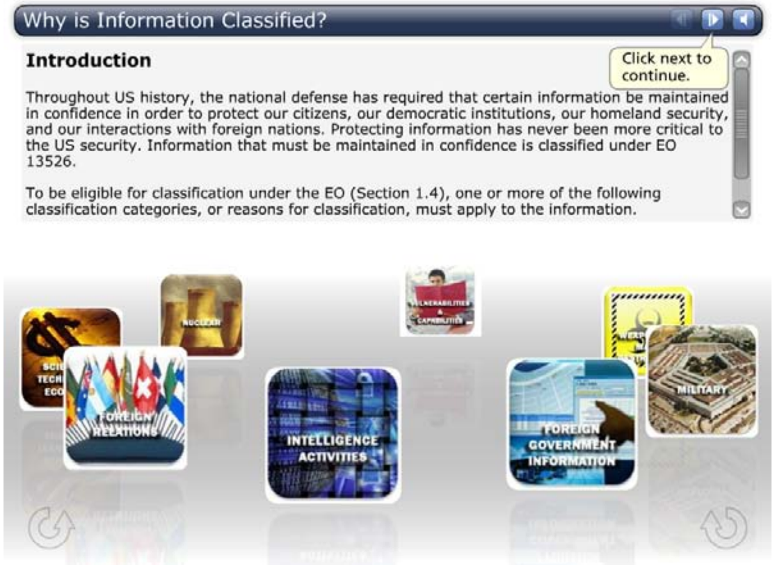
This EO establishes standard markings practices and protocols that serve to safeguard NSI and encourage responsible sharing of information across the IC; Department of Defense (DoD); Non-Title 50 organizations; state, local, tribal, and private sector entities (SLTP); as well as with US foreign partners.

(Image alt: White House building in the District of Columbia.)

ISOO Implementing Directive

The ISOO Implementing Directive, 32 CFR Part 2001 provides implementing guidance and direction for classifying, safeguarding, and declassifying NSI in accordance with EO 13526.

(Image alt: Collage of US flag, the National Archive building, emblem of National Archives and Records Administration, emblem of ISOO, and a document that states Marking Classified National Information Security.)



Why is Information Classified?

Introduction

Click next to continue.

Throughout US history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information has never been more critical to the US security. Information that must be maintained in confidence is classified under EO 13526.

To be eligible for classification under the EO (Section 1.4), one or more of the following classification categories, or reasons for classification, must apply to the information.

Why is Information Classified?

Introduction

Throughout US history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information has never been more critical to the US security. Information that must be maintained in confidence is classified under EO 13526.

To be eligible for classification under the EO (Section 1.4), one or more of the following classification categories, or reasons for classification, must apply to the information.

(Image alt: Eight reasons for classification from EO 13526 Section 1.4: military; FGI; intelligence activities; foreign relations; scientific, technical, or economic; nuclear; vulnerabilities and capabilities; and Weapons of Mass Destruction (WMD).)

Military

Military plans, weapons systems, or operations

(Image alt: The Pentagon building.)

FGI
Foreign Government Information (FGI)

(Image alt: Computer screen shots.)

Intelligence Activities
Intelligence activities (including covert action), intelligence sources or methods, or cryptology

(Image alt: Collage of global information and security.)

Foreign Relations
Foreign relations or foreign activities of the US, including confidential sources

(Image alt: Flags of many countries.)

Scientific, Technical, or Economic
Scientific, technological, or economic matters relating to national security

(Image alt: Money sign over charts and graphs.)

Nuclear
US Government programs for safeguarding nuclear materials or facilities

(Image alt: Nuclear plant cooling towers.)

Vulnerabilities and Capabilities
Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security

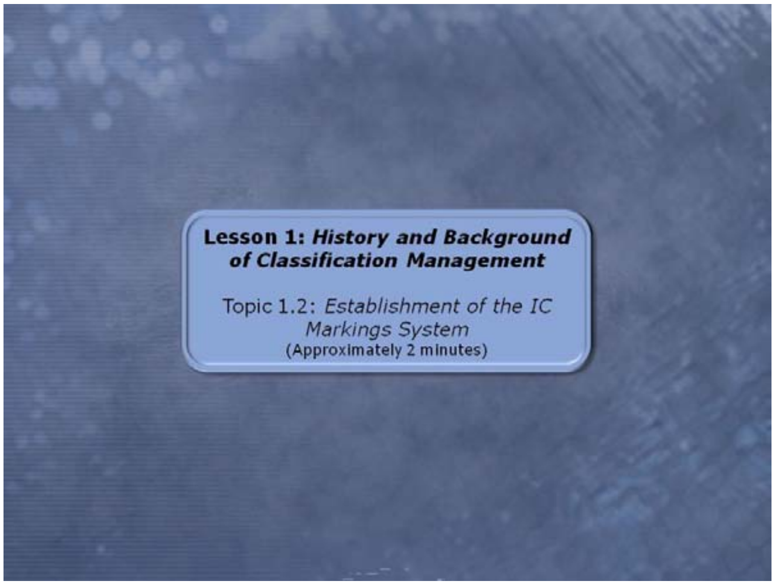
(Image alt: Man looking at plans.)

WMD
The development, production, or use of Weapons of Mass Destruction (WMD)

(Image alt: Biohazard sign.)

Summary

Senior US Government officials, delegated and authorized to make original classification decisions for their agency, use the EO classification categories to develop classification security guides in order to inform and assist personnel with classification determinations, and accurate identification and safeguarding of classified NSI.



Lesson 1: ***History and Background of Classification Management***

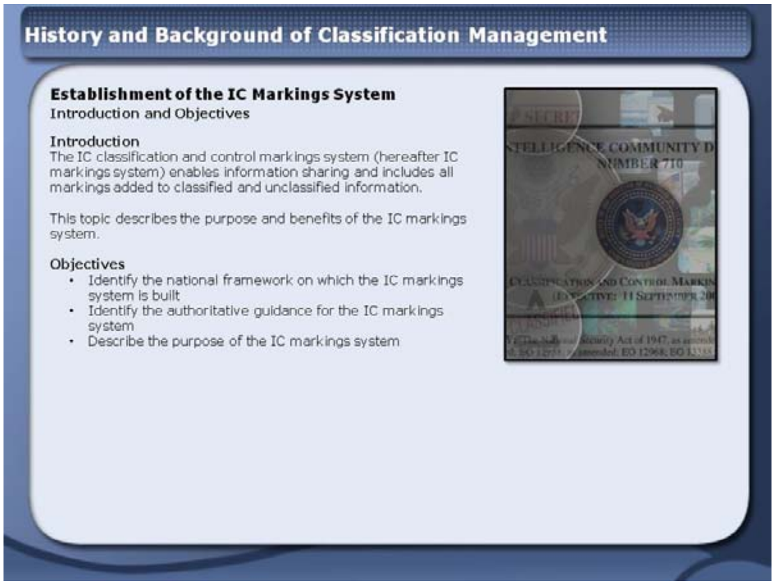
Topic 1.2: *Establishment of the IC Markings System*

(Approximately 2 minutes)

Lesson 1: *History and Background of Classification Management*

Topic 1.2: *Establishment of the IC Markings System*

(Approximately 2 minutes)



History and Background of Classification Management

Establishment of the IC Markings System

Introduction and Objectives

Introduction

The IC classification and control markings system (hereafter IC markings system) enables information sharing and includes all markings added to classified and unclassified information.

This topic describes the purpose and benefits of the IC markings system.

Objectives

- Identify the national framework on which the IC markings system is built
- Identify the authoritative guidance for the IC markings system
- Describe the purpose of the IC markings system

Introduction and Objectives

Introduction

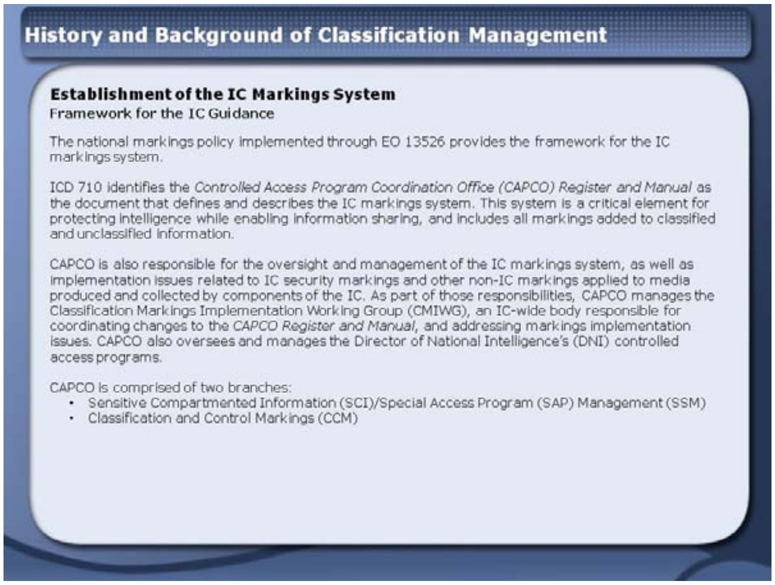
The IC classification and control markings system (hereafter IC markings system) enables information sharing and includes all markings added to classified and unclassified information.

This topic describes the purpose and benefits of the IC markings system.

Objectives

- Identify the national framework on which the IC markings system is built
- Identify the authoritative guidance for the IC markings system
- Describe the purpose of the IC markings system

(Image alt: Collage of the Office of the Director of National Intelligence (ODNI) Seals and ICD 710 document.)



History and Background of Classification Management

Establishment of the IC Markings System

Framework for the IC Guidance

The national markings policy implemented through EO 13526 provides the framework for the IC markings system.

ICD 710 identifies the *Controlled Access Program Coordination Office (CAPCO) Register and Manual* as the document that defines and describes the IC markings system. This system is a critical element for protecting intelligence while enabling information sharing, and includes all markings added to classified and unclassified information.

CAPCO is also responsible for the oversight and management of the IC markings system, as well as implementation issues related to IC security markings and other non-IC markings applied to media produced and collected by components of the IC. As part of those responsibilities, CAPCO manages the Classification Markings Implementation Working Group (CMIWG), an IC-wide body responsible for coordinating changes to the *CAPCO Register and Manual*, and addressing markings implementation issues. CAPCO also oversees and manages the Director of National Intelligence's (DNI) controlled access programs.

CAPCO is comprised of two branches:

- Sensitive Compartmented Information (SCI)/Special Access Program (SAP) Management (SSM)
- Classification and Control Markings (CCM)

Framework for the IC Guidance

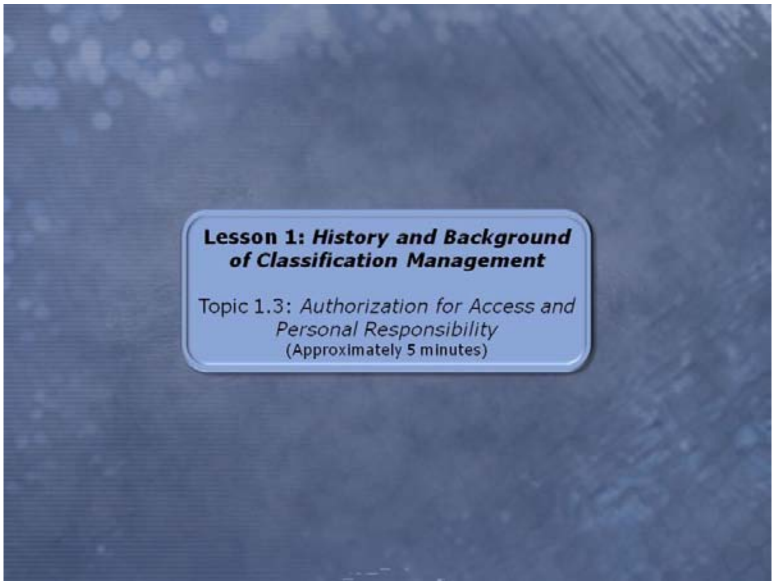
The national markings policy implemented through EO 13526 provides the framework for the IC markings system.

ICD 710 identifies the *Controlled Access Program Coordination Office (CAPCO) Register and Manual* as the document that defines and describes the IC markings system. This system is a critical element for protecting intelligence while enabling information sharing, and includes all markings added to classified and unclassified information.

CAPCO is also responsible for the oversight and management of the IC markings system, as well as implementation issues related to IC security markings and other non-IC markings applied to media produced and collected by components of the IC. As part of those responsibilities, CAPCO manages the Classification Markings Implementation Working Group (CMIWG), an IC-wide body responsible for coordinating changes to the *CAPCO Register and Manual*, and addressing markings implementation issues. CAPCO also oversees and manages the Director of National Intelligence's (DNI) controlled access programs.

CAPCO is comprised of two branches:

- Sensitive Compartmented Information (SCI)/Special Access Program (SAP) Management (SSM)
- Classification and Control Markings (CCM)



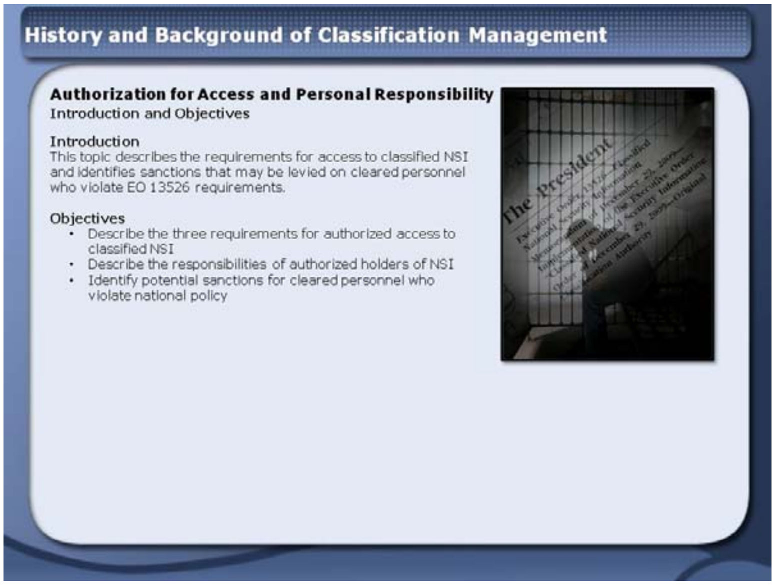
Lesson 1: ***History and Background of Classification Management***

Topic 1.3: *Authorization for Access and Personal Responsibility*
(Approximately 5 minutes)

Lesson 1: *History and Background of Classification Management*

Topic 1.3: *Authorization for Access and Personal Responsibility*

(Approximately 5 minutes)



History and Background of Classification Management

Authorization for Access and Personal Responsibility
Introduction and Objectives

Introduction
This topic describes the requirements for access to classified NSI and identifies sanctions that may be levied on cleared personnel who violate EO 13526 requirements.

Objectives
- Describe the three requirements for authorized access to classified NSI
- Describe the responsibilities of authorized holders of NSI
- Identify potential sanctions for cleared personnel who violate national policy

Introduction and Objectives

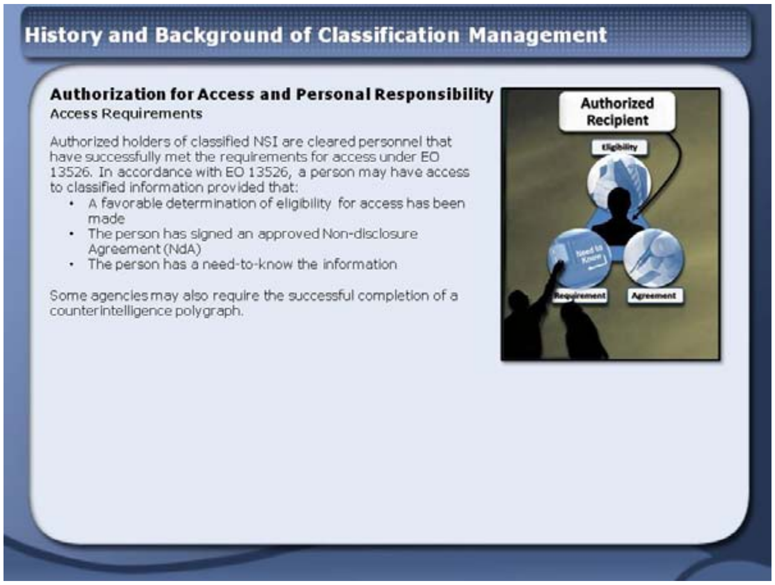
Introduction

This topic describes the requirements for access to classified NSI and identifies sanctions that may be levied on cleared personnel who violate EO 13526 requirements.

Objectives

- Describe the three requirements for authorized access to classified NSI
- Describe the responsibilities of authorized holders of NSI
- Identify potential sanctions for cleared personnel who violate national policy

(Image alt: Man sitting in jail who violated the Presidential EO.)



History and Background of Classification Management

Authorization for Access and Personal Responsibility
Access Requirements

Authorized holders of classified NSI are cleared personnel that have successfully met the requirements for access under EO 13526. In accordance with EO 13526, a person may have access to classified information provided that:
- A favorable determination of eligibility for access has been made
- The person has signed an approved Non-disclosure Agreement (NdA)
- The person has a need-to-know the information

Some agencies may also require the successful completion of a counterintelligence polygraph.

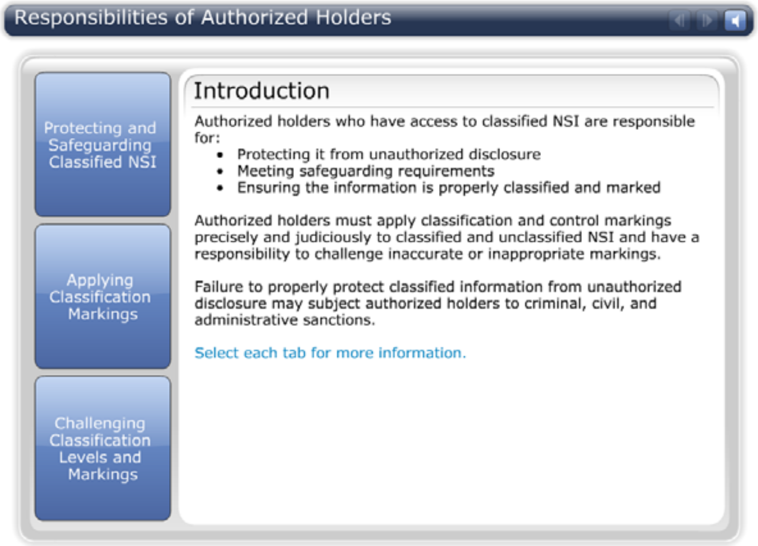
Access Requirements

Authorized holders of classified NSI are cleared personnel that have successfully met the requirements for access under EO 13526. In accordance with EO 13526, a person may have access to classified information provided that:

- A favorable determination of eligibility for access has been made
- The person has signed an approved Non-disclosure Agreement (NdA)
- The person has a need-to-know the information

Some agencies may also require the successful completion of a counterintelligence polygraph.

(Image alt: An authorized recipient has eligibility, meets requirements, and has signed an agreement.)



Responsibilities of Authorized Holders
Protecting and Safeguarding Classified NSI
Applying Classification Markings
Challenging Classification Levels and Markings

Introduction

Authorized holders who have access to classified NSI are responsible for:

- Protecting it from unauthorized disclosure
- Meeting safeguarding requirements
- Ensuring the information is properly classified and marked

Authorized holders must apply classification and control markings precisely and judiciously to classified and unclassified NSI and have a responsibility to challenge inaccurate or inappropriate markings.

Failure to properly protect classified information from unauthorized disclosure may subject authorized holders to criminal, civil, and administrative sanctions.

Select each tab for more information.

Responsibilities of Authorized Holders

Introduction

Authorized holders who have access to classified NSI are responsible for:

- Protecting it from unauthorized disclosure
- Meeting safeguarding requirements
- Ensuring the information is properly classified and marked

Authorized holders must apply classification and control markings precisely and judiciously to classified and unclassified NSI and have a responsibility to challenge inaccurate or inappropriate markings.

Failure to properly protect classified information from unauthorized disclosure may subject authorized holders to criminal, civil, and administrative sanctions.

Protecting and Safeguarding Classified NSI

Authorized holders of NSI are responsible for protecting NSI in accordance with national policy and individual agency guidance.

Authorized holders must ensure classified and controlled NSI is not disclosed or inadvertently intercepted by unauthorized recipients; this includes Controlled Unclassified Information (CUI), which may be extremely sensitive. In addition, wholly unclassified NSI must not be communicated with unauthorized persons, as it is government-owned and must be reviewed prior to disclosure or release.

Your agency security officer, classification management representative, or information management officer can provide specific guidance on proper protection requirements for all forms of NSI.

(Image alt: Protecting and Safeguarding Classified NSI - a pad lock, key, secure bag, and a secure file cabinet protecting and safeguarding classified NSI.)

Applying classification Markings

To support an integrated, collaborative, and sharing enterprise, authorized holders are responsible for applying classification and control markings precisely and judiciously to information to ensure that recipients understand how to protect the information and make informed decisions regarding dissemination and sharing. Additionally, IC personnel are responsible for applying markings that support intelligence production principles, to include writing for maximum utility.

(Image alt: Applying Classification Markings – an authorized holder ensuring information is properly classified and marked.)

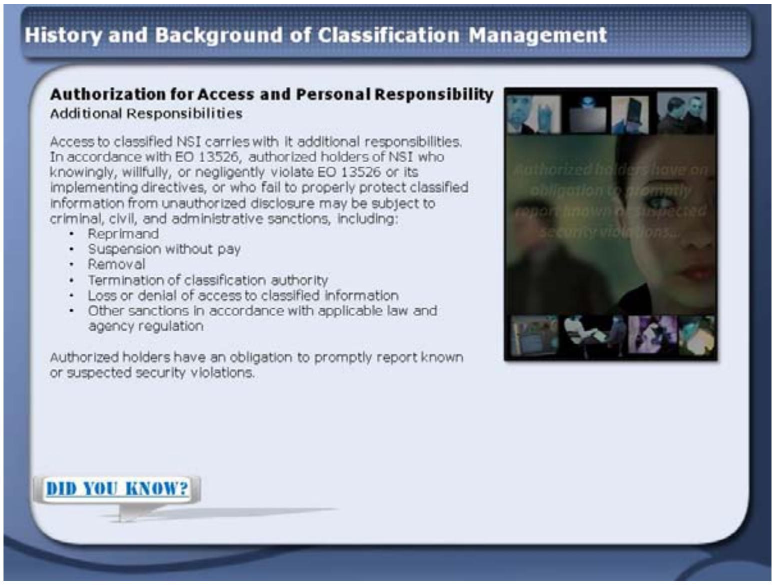
Challenging Classification Levels and Markings

Classification challenges promote proper and thoughtful classification, ensure the integrity of classification processes, support effective sharing practices, and improve marking standards. As such, authorized holders who wish to challenge a classification status or the accuracy of markings, are encouraged to do so.

Informal challenges - such as directly contacting the classifier for clarification - should be considered as a first course of action to hold down the number of formal challenges. Formal challenges must be presented in writing to an Original Classification Authority (OCA) with jurisdiction over the information.

NOTE: Authorized holders who bring forward a challenge in good faith are not subject to retribution. Your agency security officer, classification management representative, or information management officer can provide further guidance on classification and markings challenge procedures.

(Image alt: Challenging Classification Levels and Markings – documents being reviewed for classification challenges.)



History and Background of Classification Management

Authorization for Access and Personal Responsibility

Additional Responsibilities

Access to classified NSI carries with it additional responsibilities. In accordance with EO 13526, authorized holders of NSI who knowingly, willfully, or negligently violate EO 13526 or its implementing directives, or who fail to properly protect classified information from unauthorized disclosure may be subject to criminal, civil, and administrative sanctions, including:

- Reprimand
- Suspension without pay
- Removal
- Termination of classification authority
- Loss or denial of access to classified information
- Other sanctions in accordance with applicable law and agency regulation

Authorized holders have an obligation to promptly report known or suspected security violations.

Authorized holders have an obligation to promptly report known or suspected security violations...
DID YOU KNOW?

Additional Responsibilities

Access to classified NSI carries with it additional responsibilities. In accordance with EO 13526, authorized holders of NSI who knowingly, willfully, or negligently violate EO 13526 or its implementing directives, or who fail to properly protect classified information from unauthorized disclosure may be subject to criminal, civil, and administrative sanctions, including:

- Reprimand
- Suspension without pay
- Removal
- Termination of classification authority
- Loss or denial of access to classified information
- Other sanctions in accordance with applicable law and agency regulation

Authorized holders have an obligation to promptly report known or suspected security violations.

Pop Up: Did You Know?
As an authorized holder, it is your responsibility to ensure that NSI is properly marked and protected so that it does not fall into the hands of an unauthorized recipient.

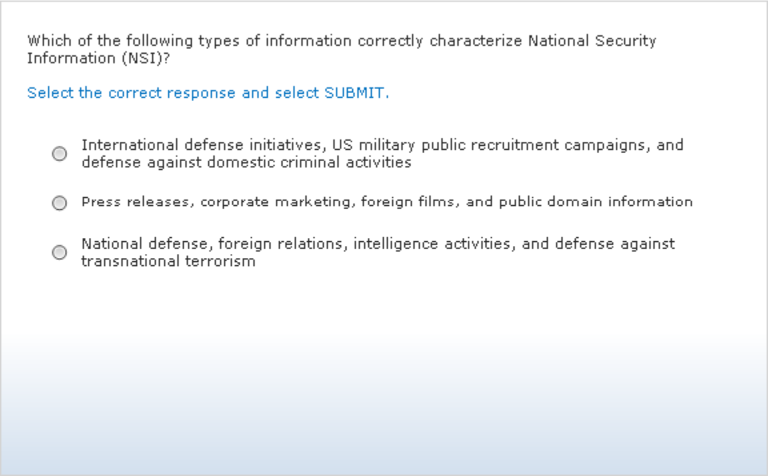
(Image alt: Women and other authorized holders reporting suspected security violations.)

Lesson 1 Knowledge Check

Introduction

The knowledge check consists of 9 questions.
(Approximately 10 minutes)

NOTE: All examples are notional and are marked for training purposes only.



Which of the following types of information correctly characterize National Security Information (NSI)?

Select the correct response and select SUBMIT.

○ International defense initiatives, US military public recruitment campaigns, and defense against domestic criminal activities

○ Press releases, corporate marketing, foreign films, and public domain information

○ National defense, foreign relations, intelligence activities, and defense against transnational terrorism

Topic 1.1

1 of 9: Which of the following types of information correctly characterize National Security Information (NSI)?

Select the correct response and continue reading for correct and incorrect feedback.

- International defense initiatives, US military public recruitment campaigns, and defense against domestic criminal activities
- Press releases, corporate marketing, foreign films, and public domain information
- National defense, foreign relations, intelligence activities, and defense against transnational terrorism

The correct answer is:

- National defense, foreign relations, intelligence activities, and defense against transnational terrorism

Feedback when correct:

That's right! National defense, foreign relations, intelligence activities, and defense against transnational terrorism all correctly characterize NSI.

Feedback when incorrect:

You did not select the correct response. The correct response is national defense, foreign relations, intelligence activities, and defense against transnational terrorism.

2 of 9: Which of the following are key National policies that provide the necessary guidance on identifying, handling, and marking National Security Information (NSI)?

Select all that apply and continue reading for correct and incorrect feedback.

- *EO 13526, Classified National Security Information*
- *32 CFR Part 2001, ISOO Implementing Directive*
- *ICD 710, Classification and Control Markings System*

The correct answers are:

- *EO 13526, Classified National Security Information*
- *32 CFR Part 2001, ISOO Implementing Directive*

Feedback when correct:

That's right! *EO 13526, Classified National Security Information* and *32 CFR Part 2001, ISOO Implementing Directive* are key National policies that provide the necessary guidance on identifying, handling, and marking NSI.

Feedback when incorrect:

You did not select the correct responses. The correct responses are:

- *EO 13526, Classified National Security Information*
- *32 CFR Part 2001, ISOO Implementing Directive*

EO 13526, Classified National Security Information and *32 CFR Part 2001, ISOO Implementing Directive* are key National policies that provide the necessary guidance on identifying, handling, and marking NSI.

3 of 9: Which of the following are reasons for classifying information?

Select all that apply and continue reading for correct and incorrect feedback.

- The development, production, or use of Weapons of Mass Destruction (WMD)
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
- Military plans, weapons systems, or operations
- Foreign Government Information (FGI)
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology

The correct choices are:

- The development, production, or use of Weapons of Mass Destruction (WMD)
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
- Military plans, weapons systems, or operations
- Foreign Government Information (FGI)
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology

Feedback when correct:

That's right! The reasons for classifying information are:

- The development, production, or use of Weapons of Mass Destruction (WMD)
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
- Military plans, weapons systems, or operations
- Foreign Government Information (FGI)
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology

In addition, there are three more reasons for classifying information:

- Foreign relations or foreign activities of the US, including confidential sources
- Scientific, technological, or economic matters relating to the national security
- US Government programs for safeguarding nuclear materials or facilities

Feedback when incorrect:

You did not select the correct responses. The correct responses are:

- The development, production, or use of Weapons of Mass Destruction (WMD)
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
- Military plans, weapons systems, or operations
- Foreign Government Information (FGI)
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology

In addition, there are three more reasons for classifying information:

- Foreign relations or foreign activities of the US, including confidential sources
- Scientific, technological, or economic matters relating to the national security
- US Government programs for safeguarding nuclear materials or facilities

Topic 1.2

4 of 9: The national markings policy on classifying, safeguarding, and declassifying National Security Information (NSI) implemented through EO 13526 provides the framework for the IC guidance.

Select True or False and continue reading for correct and incorrect feedback.

- True
- False

The correct answer is “True.”

Feedback when correct:
That's right! The national markings policy on classifying, safeguarding, and declassifying National Security Information (NSI) implemented through EO 13526 provides the framework for the IC guidance.

Feedback when incorrect:
You did not select the correct response. The correct response is “True.”

The national markings policy on classifying, safeguarding, and declassifying National Security Information (NSI) implemented through EO 13526 provides the framework for the IC guidance.

5 of 9: What guidance defines and describes the IC markings system?

Select the correct response and continue reading for correct and incorrect feedback.

- ICD 710
- EO 13526
- *CAPCO Register and Manual*
- None of the above

The correct answer is "*CAPCO Register and Manual.*"

Feedback when correct:
That's right! The guidance that defines and describes the IC markings system is the *CAPCO Register and Manual*. ICD 710 establishes this document as the IC markings system.

Feedback when incorrect:
You did not select the correct response. The correct response is the *CAPCO Register and Manual.*

The guidance that defines and describes the IC markings system is the *CAPCO Register and Manual. ICD* 710 establishes this document as the IC markings system.

6 of 9: The IC markings system is a critical element of IC procedures for protecting intelligence, and sources and methods, while enabling information sharing and includes all markings added to classified and unclassified information.

Select True or False and continue reading for correct and incorrect feedback.

- True
- False

The correct answer is “True.”

Feedback when correct:
That's right! The IC markings system is a critical element of IC procedures for protecting intelligence, and sources and methods, while enabling information sharing and includes all markings added to classified and unclassified information.

Feedback when incorrect:
You did not select the correct response. The correct response is “True.”

The IC markings system is a critical element of IC procedures for protecting intelligence, and sources and methods, while enabling information sharing and includes all markings added to classified and unclassified information.

Topic 1.3
7 of 9: A person may have access to classified information when which of the following requirements are met?

Select the correct response and continue reading for correct and incorrect feedback.

- A favorable determination of eligibility for access has been made
- The person has signed an approved Non-disclosure Agreement (NdA)
- The person has a need-to-know the information
- All of the above

The correct answer is "All of the above."

Feedback when correct:

That's right! A person may have access to classified information provided that all of the following apply:

- A favorable determination of eligibility for access has been made
- The person has signed an approved Non-disclosure Agreement (NdA)
- The person has a need-to-know the information

Feedback when incorrect:

You did not select the correct response. The correct response is: "All of the above."

A person may have access to classified information provided that all of the following apply:

- A favorable determination of eligibility for access has been made
- The person has signed an approved Non-disclosure Agreement (NdA)
- The person has a need-to-know the information

8 of 9: What are the responsibilities of authorized holders who have access to classified National Security Information (NSI)?

Select the correct response and continue reading for correct and incorrect feedback.

- Protecting NSI from persons that do not have authorized access to that information
- Meeting safeguarding requirements prescribed by the agency head
- Ensuring that classified information is not disclosed or inadvertently intercepted by unauthorized persons
- Properly marking and safeguarding NSI in accordance with EO 13526, the Implementing Directive (32 CFR Part 2001), and Intelligence Community Directive (ICD) 710.
- All of the above

The correct answer is “All of the above.”

Feedback when correct:
That's right!

Authorized holders who have access to classified NSI are responsible for all of the following:

- Protecting NSI from persons that do not have authorized access to that information
- Meeting safeguarding requirements prescribed by the agency head
- Ensuring that classified information is not disclosed or inadvertently intercepted by unauthorized persons
- Properly marking and safeguarding NSI in accordance with EO 13526, the Implementing Directive (32 CFR Part 2001), and ICD 710

Feedback when incorrect:
You did not select the correct response. The correct response is: "All of the above."

Authorized holders who have access to classified NSI are responsible for all of the following:

- Protecting NSI from persons that do not have authorized access to that information
- Meeting safeguarding requirements prescribed by the agency head
- Ensuring that classified information is not disclosed or inadvertently intercepted by unauthorized persons
- Properly marking and safeguarding NSI in accordance with EO 13526, the Implementing Directive (32 CFR Part 2001), and ICD 710

9 of 9: Authorized holders of National Security Information (NSI) who knowingly, willfully, or negligently violate EO 13526 or its implementing directives, or who fail to properly protect classified information from unauthorized disclosure may be subject to criminal, civil, and administrative sanctions, including:

- **Suspension without pay**
- **Removal**
- **Loss or denial of access to classified information**

Select True or False and continue reading for correct and incorrect feedback.

- True
- False

The correct answer is “True”.

Feedback when correct:
That's right!

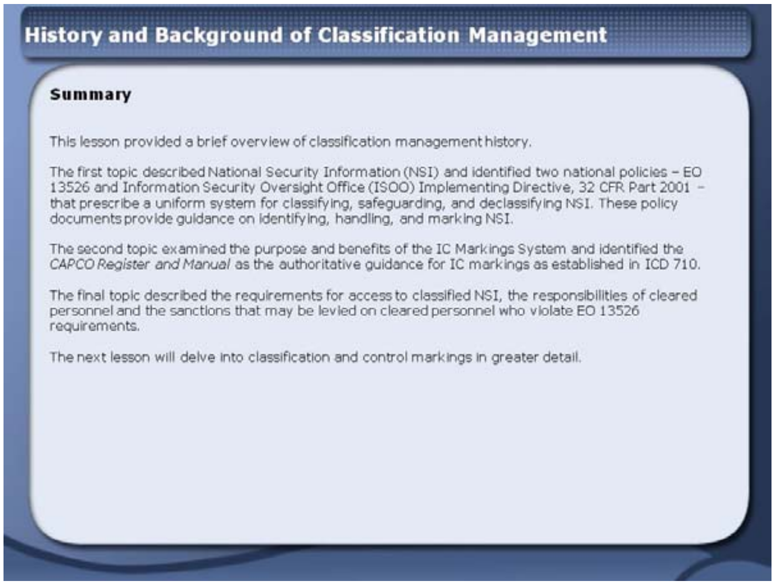
Other criminal, civil, and administrative sanctions, the violator may face include:

- Reprimand
- Termination of classification authority
- Other sanctions in accordance with applicable law and agency regulation

Feedback when incorrect:
You did not select the correct response. The correct response is “True.”

Other criminal, civil, and administrative sanctions, the violator may face include:

- Reprimand
- Termination of classification authority
- Other sanctions in accordance with applicable law and agency regulation



History and Background of Classification Management

Summary

This lesson provided a brief overview of classification management history.

The first topic described National Security Information (NSI) and identified two national policies – EO 13526 and Information Security Oversight Office (ISOO) Implementing Directive, 32 CFR Part 2001 – that prescribe a uniform system for classifying, safeguarding, and declassifying NSI. These policy documents provide guidance on identifying, handling, and marking NSI.

The second topic examined the purpose and benefits of the IC Markings System and identified the *CAPCO Register and Manual* as the authoritative guidance for IC markings as established in ICD 710.

The final topic described the requirements for access to classified NSI, the responsibilities of cleared personnel and the sanctions that may be levied on cleared personnel who violate EO 13526 requirements.

The next lesson will delve into classification and control markings in greater detail.

Summary

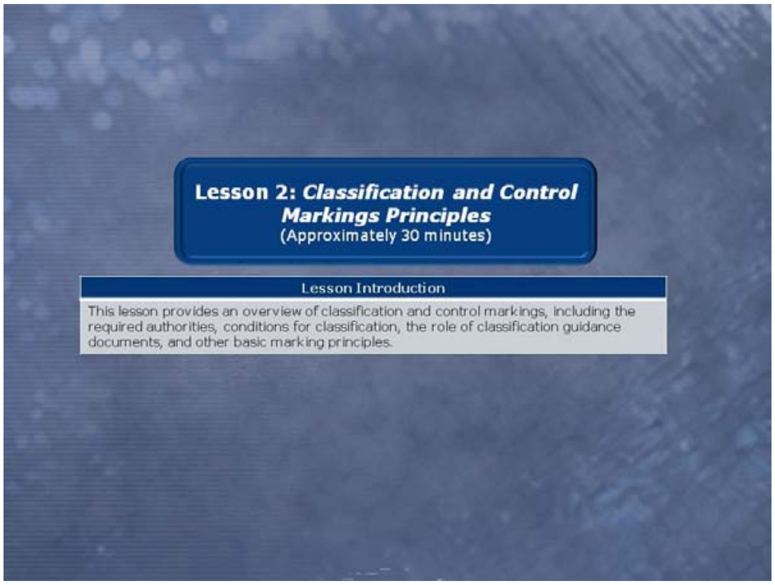
This lesson provided a brief overview of classification management history.

The first topic described National Security Information (NSI) and identified two national policies – EO 13526 and Information Security Oversight Office (ISOO) Implementing Directive, 32 CFR Part 2001 – that prescribe a uniform system for classifying, safeguarding, and declassifying NSI. These policy documents provide guidance on identifying, handling, and marking NSI.

The second topic examined the purpose and benefits of the IC Markings System and identified the *CAPCO Register and Manual* as the authoritative guidance for IC markings as established in ICD 710.

The final topic described the requirements for access to classified NSI, the responsibilities of cleared personnel and the sanctions that may be levied on cleared personnel who violate EO 13526 requirements.

The next lesson will delve into classification and control markings in greater detail.



Lesson 2: *Classification and Control Markings Principles*
(Approximately 30 minutes)

Lesson Introduction

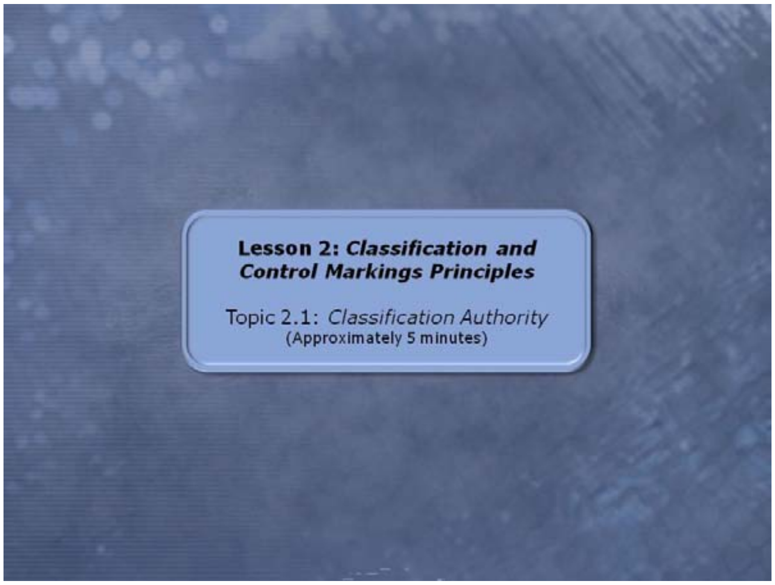
This lesson provides an overview of classification and control markings, including the required authorities, conditions for classification, the role of classification guidance documents, and other basic marking principles.

Lesson 2: *Classification and Control Markings Principles*

(Approximately 30 minutes)

Lesson Introduction

This lesson provides an overview of classification and control markings, including the required authorities, conditions for classification, the role of classification guidance documents, and other basic marking principles.



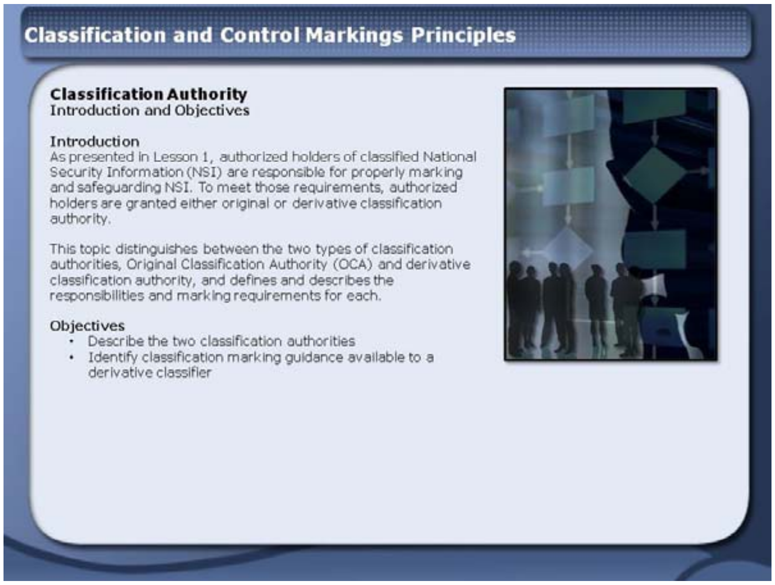
Lesson 2: *Classification and Control Markings Principles*

Topic 2.1: *Classification Authority*
(Approximately 5 minutes)

Lesson 2: *Classification and Control Markings Principles*

Topic 2.1: *Classification Authority*

(Approximately 5 minutes)



Classification and Control Markings Principles

Classification Authority
Introduction and Objectives

Introduction
As presented in Lesson 1, authorized holders of classified National Security Information (NSI) are responsible for properly marking and safeguarding NSI. To meet those requirements, authorized holders are granted either original or derivative classification authority.

This topic distinguishes between the two types of classification authorities, Original Classification Authority (OCA) and derivative classification authority, and defines and describes the responsibilities and marking requirements for each.

Objectives
- Describe the two classification authorities
- Identify classification marking guidance available to a derivative classifier

Introduction and Objectives

Introduction

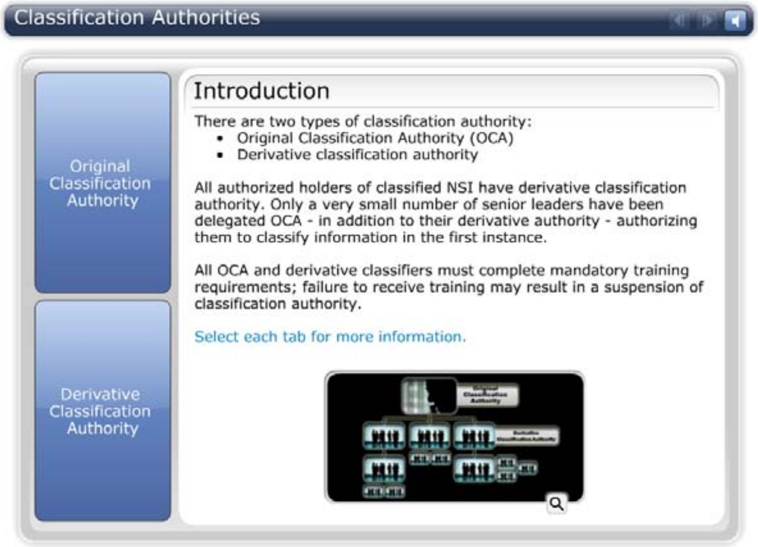
As presented in Lesson 1, authorized holders of classified National Security Information (NSI) are responsible for properly marking and safeguarding NSI. To meet those requirements, authorized holders are granted either original or derivative classification authority.

This topic distinguishes between the two types of classification authorities, Original Classification Authority (OCA) and derivative classification authority, and defines and describes the responsibilities and marking requirements for each.

Objectives

- Describe the two classification authorities
- Identify classification marking guidance available to a derivative classifier

(Image alt: Group of people and flow charts.)


Classification Authorities
Original Classification Authority
Derivative Classification Authority

Introduction

There are two types of classification authority:

- Original Classification Authority (OCA)
- Derivative classification authority

All authorized holders of classified NSI have derivative classification authority. Only a very small number of senior leaders have been delegated OCA - in addition to their derivative authority - authorizing them to classify information in the first instance.

All OCA and derivative classifiers must complete mandatory training requirements; failure to receive training may result in a suspension of classification authority.

Select each tab for more information.

Classification Authorities

Introduction

There are two types of classification authority:

- Original Classification Authority (OCA)
- Derivative classification authority

All authorized holders of classified NSI have derivative classification authority. Only a very small number of senior leaders have been delegated OCA - in addition to their derivative authority - authorizing them to classify information in the first instance.

All OCA and derivative classifiers must complete mandatory training requirements; failure to receive training may result in a suspension of classification authority.

(Image alt: Flow chart with groups of people representing two types of classification authorities: OCA and Derivative classification of authority.)

Original Classification Authority

OCAs are senior government officials with expert knowledge of their respective organizations, enabling them to make determinations about risk and expected damage to national security should the information be disclosed without proper authorization.

To make these determinations, OCAs must have jurisdiction over the information they are classifying for the first time, and must be able to:

- Identify one or more of the eight categories (reasons for classification) of NSI described in Section 1.4 of EO 13526

- Describe the damage to national security (classification level) that is expected to occur should the information be improperly disclosed
- Describe the appropriate duration of classification (declassification instructions)

Classification guides are agency or program-specific and are authorized by OCAs with jurisdiction over the information. They facilitate the proper and uniform derivative classification of information and serve as a primary resource for classification determinations made by derivative classification authorities.

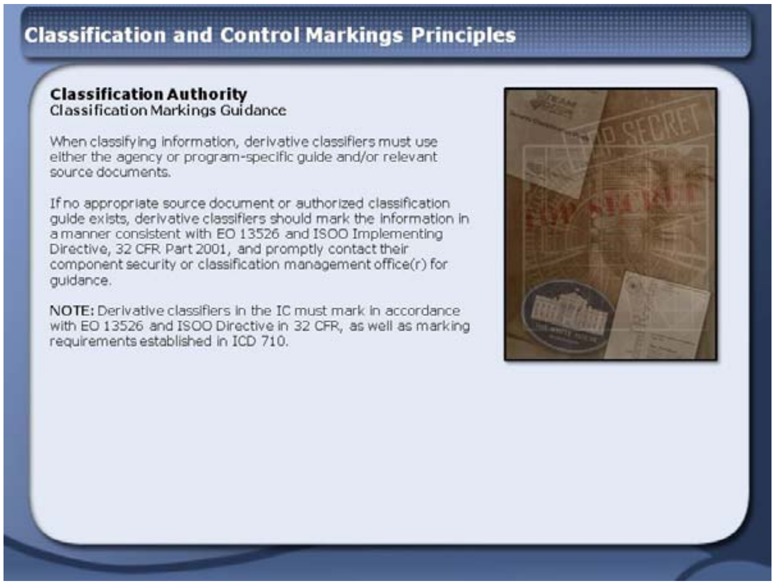
Derivative Classification Authority

Derivative classification authorities are authorized holders of classified information in a given agency. Derivative classifiers reproduce, extract, and summarize classified information. In other words, derivative classifiers apply classification markings **derived** from source material or as directed by a classification guide.

Derivative classifiers must observe and respect original classification decisions, including OCA-authorized classification guides.

When properly developed, guides:

- Facilitate the proper and uniform derivative classification of information
- Identify the discreet elements of classified information by subject and establish the level and duration of classification for each element
- Identify additional control markings necessary to protect the elements of information from unauthorized disclosure
- Provide appropriate durations for classification of the information



Classification and Control Markings Principles

Classification Authority
Classification Markings Guidance

When classifying information, derivative classifiers must use either the agency or program-specific guide and/or relevant source documents.

If no appropriate source document or authorized classification guide exists, derivative classifiers should mark the information in a manner consistent with EO 13526 and ISOO Implementing Directive, 32 CFR Part 2001, and promptly contact their component security or classification management office(r) for guidance.

NOTE: Derivative classifiers in the IC must mark in accordance with EO 13526 and ISOO Directive in 32 CFR, as well as marking requirements established in ICD 710.

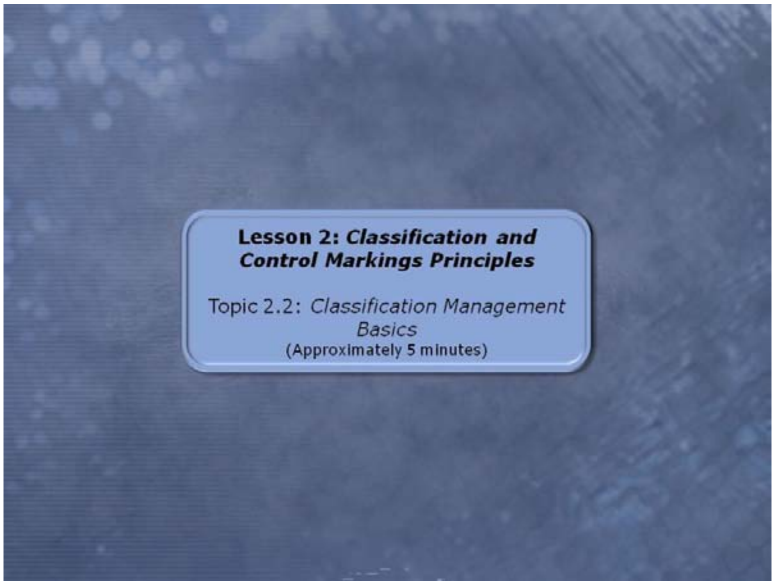
Classification Markings Guidance

When classifying information, derivative classifiers must use either the agency or program-specific guide and/or relevant source documents.

If no appropriate source document or authorized classification guide exists, derivative classifiers should mark the information in a manner consistent with EO 13526 and ISOO Implementing Directive, 32 CFR Part 2001, and promptly contact their component security or classification management office(r) for guidance.

NOTE: Derivative classifiers in the IC must mark in accordance with EO 13526 and ISOO Directive in 32 CFR, as well as marking requirements established in ICD 710.

(Image alt: Collage of EO 13526, White House, and President Roosevelt.)



Lesson 2: ***Classification and Control Markings Principles***

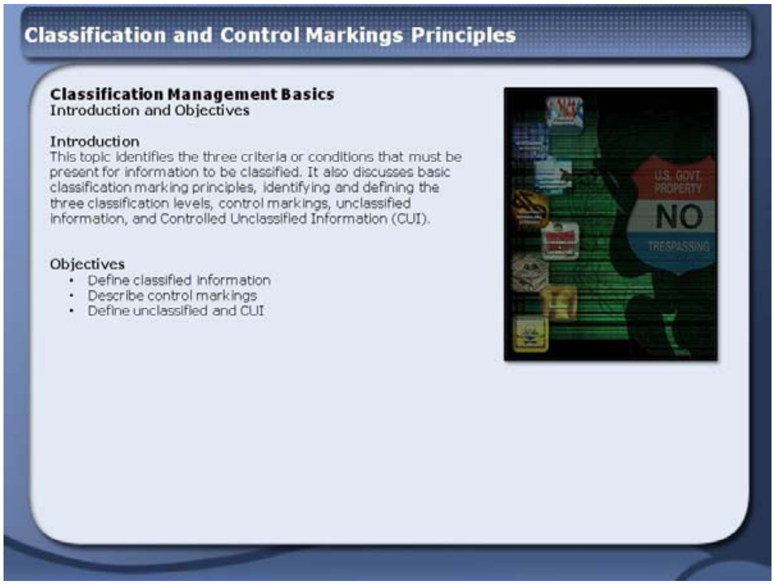
Topic 2.2: *Classification Management Basics*

(Approximately 5 minutes)

Lesson 2: *Classification and Control Markings Principles*

Topic 2.2: *Classification Management Basics*

(Approximately 5 minutes)



Classification and Control Markings Principles

Classification Management Basics
Introduction and Objectives

Introduction
This topic identifies the three criteria or conditions that must be present for information to be classified. It also discusses basic classification marking principles, identifying and defining the three classification levels, control markings, unclassified information, and Controlled Unclassified Information (CUI).

Objectives

- Define classified information
- Describe control markings
- Define unclassified and CUI

Introduction and Objectives

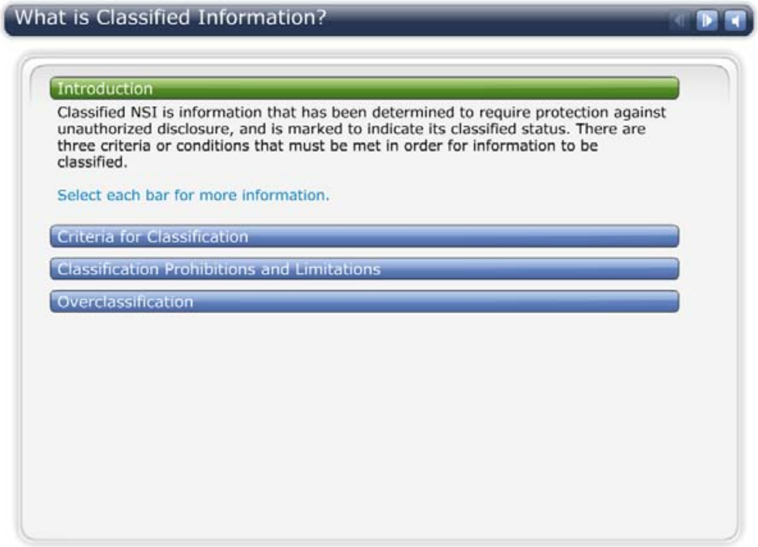
Introduction

This topic identifies the three criteria or conditions that must be present for information to be classified. It also discusses basic classification marking principles, identifying and defining the three classification levels, control markings, unclassified information, and Controlled Unclassified Information (CUI).

Objectives

- Define classified information
- Describe control markings
- Define unclassified and CUI

(Image alt: Collage of US Government Property: No Trespassing, a man keeping a secret, and various elements of classified information.)


What is Classified Information?
Introduction
Criteria for Classification
Classification Prohibitions and Limitations
Overclassification

Classified NSI is information that has been determined to require protection against unauthorized disclosure, and is marked to indicate its classified status. There are three criteria or conditions that must be met in order for information to be classified.

Select each bar for more information.

What is Classified Information?

Introduction

Classified NSI is information that has been determined to require protection against unauthorized disclosure, and is marked to indicate its classified status. There are three criteria or conditions that must be met in order for information to be classified.

Criteria for Classification

Information may be classified if the following three criteria are met:

- The information is owned by, produced by or for, or is under the control of the US Government
- The information meets one or more of the categories of information in section 1.4 of EO 13526
- The OCA who classifies the information in the first instance, determines that unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the OCA is able to identify or describe the damage

Classification Prohibitions and Limitations

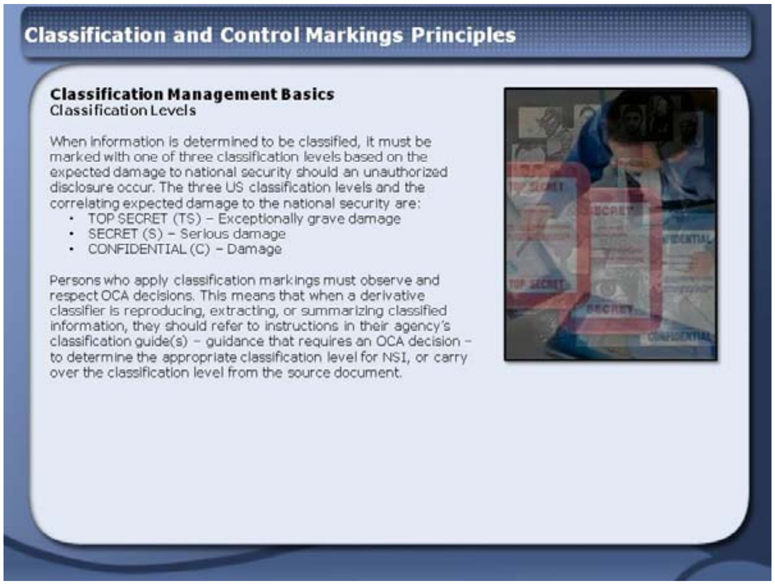
Information shall not be classified in order to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of the national security

Overclassification

Avoid overclassification by using the following rules:

- When there is significant doubt about the appropriate level of classification, information shall be classified at the lower level
- When there is significant doubt as to whether the information should be classified, it shall not be classified



Classification and Control Markings Principles

Classification Management Basics
Classification Levels

When information is determined to be classified, it must be marked with one of three classification levels based on the expected damage to national security should an unauthorized disclosure occur. The three US classification levels and the correlating expected damage to the national security are:

- TOP SECRET (TS) – Exceptionally grave damage
- SECRET (S) – Serious damage
- CONFIDENTIAL (C) – Damage

Persons who apply classification markings must observe and respect OCA decisions. This means that when a derivative classifier is reproducing, extracting, or summarizing classified information, they should refer to instructions in their agency's classification guide(s) – guidance that requires an OCA decision – to determine the appropriate classification level for NSI, or carry over the classification level from the source document.

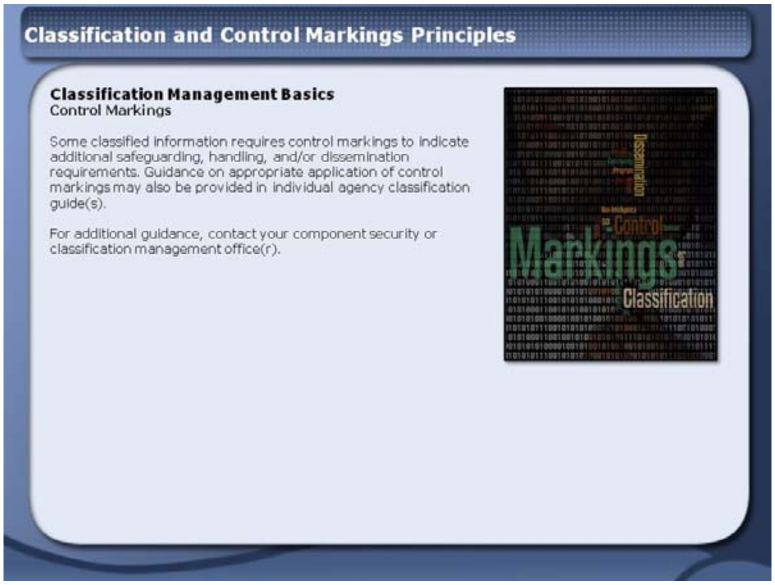
Classification Levels

When information is determined to be classified, it must be marked with one of three classification levels based on the expected damage to national security should an unauthorized disclosure occur. The three US classification levels and the correlating expected damage to the national security are:

- TOP SECRET (TS) – Exceptionally grave damage
- SECRET (S) – Serious damage
- CONFIDENTIAL (C) – Damage

Persons who apply classification markings must observe and respect OCA decisions. This means that when a derivative classifier is reproducing, extracting, or summarizing classified information, they should refer to instructions in their agency's classification guide(s) – guidance that requires an OCA decision – to determine the appropriate classification level for NSI, or carry over the classification level from the source document.

(Image alt: A man working on marking documents with the classification levels: TOP SECRET, SECRET, and CONFIDENTIAL.)



Classification and Control Markings Principles

Classification Management Basics
Control Markings

Some classified information requires control markings to indicate additional safeguarding, handling, and/or dissemination requirements. Guidance on appropriate application of control markings may also be provided in individual agency classification guide(s).

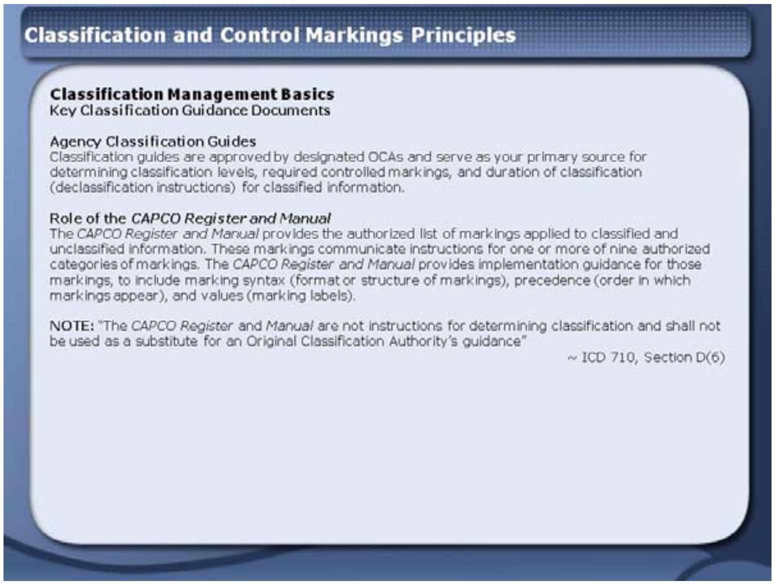
For additional guidance, contact your component security or classification management office(r).

Control Markings

Some classified information requires control markings to indicate additional safeguarding, handling, and/or dissemination requirements. Guidance on appropriate application of control markings may also be provided in individual agency classification guide(s).

For additional guidance, contact your component security or classification management office(r).

(Image alt: Image of the words markings, dissemination, classification, and control.)



Classification and Control Markings Principles

Classification Management Basics
Key Classification Guidance Documents

Agency Classification Guides
Classification guides are approved by designated OCAs and serve as your primary source for determining classification levels, required controlled markings, and duration of classification (declassification instructions) for classified information.

Role of the *CAPCO Register and Manual*
The *CAPCO Register and Manual* provides the authorized list of markings applied to classified and unclassified information. These markings communicate instructions for one or more of nine authorized categories of markings. The *CAPCO Register and Manual* provides implementation guidance for those markings, to include marking syntax (format or structure of markings), precedence (order in which markings appear), and values (marking labels).

NOTE: "The *CAPCO Register* and *Manual* are not instructions for determining classification and shall not be used as a substitute for an Original Classification Authority's guidance"
~ ICD 710, Section D(6)

Key Classification Guidance Documents

Agency Classification Guides

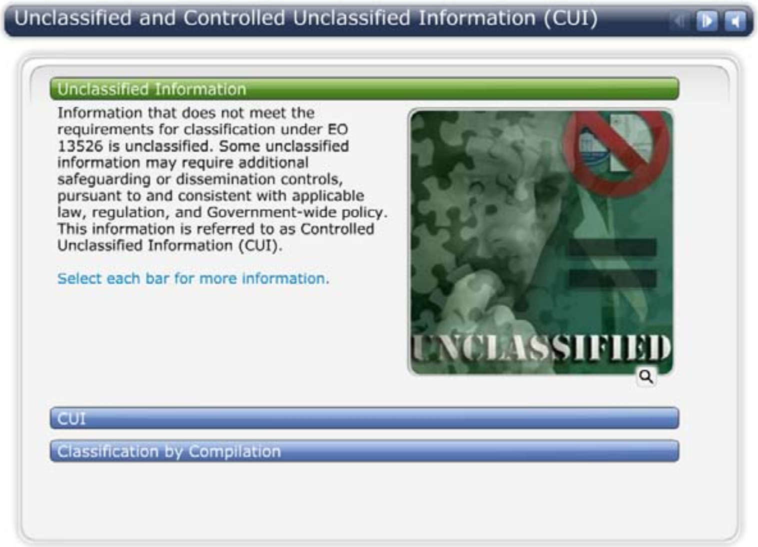
Classification guides are approved by designated OCAs and serve as your primary source for determining classification levels, required controlled markings, and duration of classification (declassification instructions) for classified information.

Role of the *CAPCO Register and Manual*

The *CAPCO Register and Manual* provides the authorized list of markings applied to classified and unclassified information. These markings communicate instructions for one or more of nine authorized categories of markings. The *CAPCO Register and Manual* provides implementation guidance for those markings, to include marking syntax (format or structure of markings), precedence (order in which markings appear), and values (marking labels).

NOTE: "The *CAPCO Register* and *Manual* are not instructions for determining classification and shall not be used as a substitute for an Original Classification Authority's guidance"

~ ICD 710, Section D(6)



Unclassified and Controlled Unclassified Information (CUI)
Unclassified Information
UNCLASSIFIED
CUI
Classification by Compilation

Information that does not meet the requirements for classification under EO 13526 is unclassified. Some unclassified information may require additional safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulation, and Government-wide policy. This information is referred to as Controlled Unclassified Information (CUI).

Select each bar for more information.

Unclassified and Controlled Unclassified Information (CUI)

Unclassified Information

Information that does not meet the requirements for classification under EO 13526 is unclassified. Some unclassified information may require additional safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulation, and Government-wide policy. This information is referred to as Controlled Unclassified Information (CUI).

(Image alt: Image of a man thinking, the EO crossed out, an equals sign, and the word UNCLASSIFIED.)

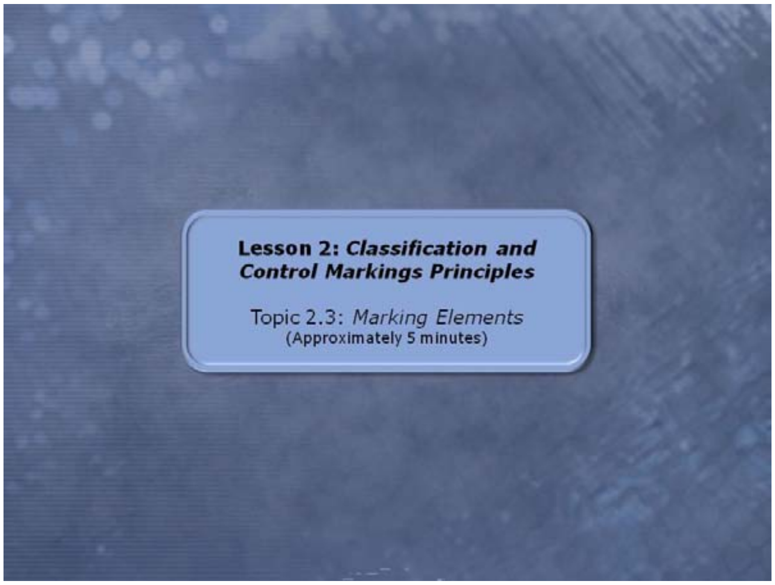
CUI
The CUI program was established on November 4, 2010 with the signing of *EO 13556*, *Controlled Unclassified Information*. The EO emphasizes openness and uniformity (standardization) to manage unclassified information that requires safeguarding or dissemination controls.

The program has not been fully implemented and CUI markings have not yet been established. CUI markings shall not be applied until formally directed by your agency to do so. Direct questions regarding CUI markings to your component security or classification management office(r).

(Image alt: A picture of President Obama with text of EO 13556.)

Classification by Compilation
Information that individually is unclassified or classified at a lower level, may become classified or classified at a higher level when aggregated or compiled in a single document, if the compiled information reveals an additional association or relationship that meets the standards for classification under EO 13526.

(Image alt: Image of puzzle pieces all labeled FOR OFFICIAL USE ONLY (FOUO).)



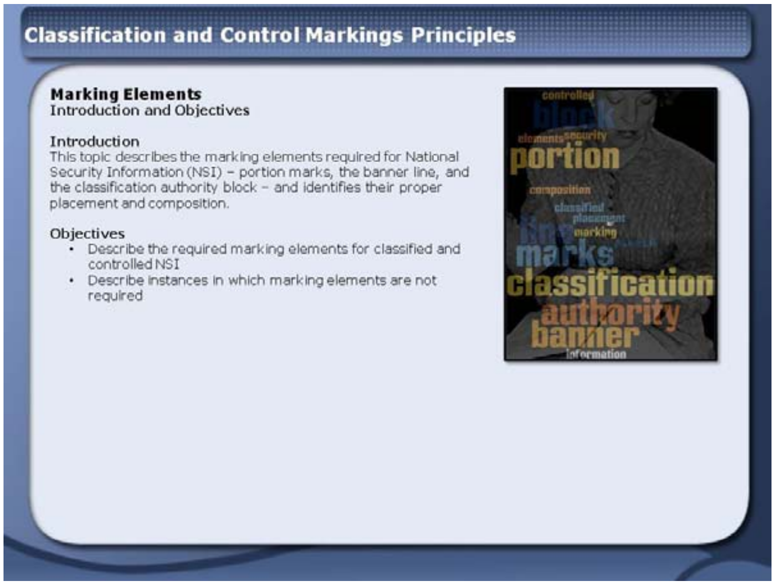
Lesson 2: ***Classification and Control Markings Principles***

Topic 2.3: *Marking Elements*
(Approximately 5 minutes)

Lesson 2: *Classification and Control Markings Principles*

Topic 2.3: *Marking Elements*

(Approximately 5 minutes)



Classification and Control Markings Principles

Marking Elements
Introduction and Objectives

Introduction
This topic describes the marking elements required for National Security Information (NSI) – portion marks, the banner line, and the classification authority block – and identifies their proper placement and composition.

Objectives

- Describe the required marking elements for classified and controlled NSI
- Describe instances in which marking elements are not required

Introduction and Objectives

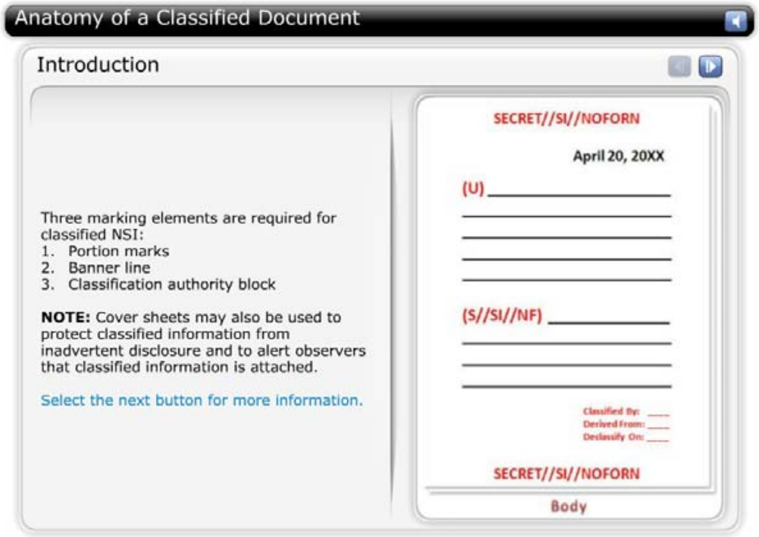
Introduction

This topic describes the marking elements required for National Security Information (NSI) – portion marks, the banner line, and the classification authority block – and identifies their proper placement and composition.

Objectives

- Describe the required marking elements for classified and controlled NSI
- Describe instances in which marking elements are not required

(Image alt: A women adding marking elements to a document with markings-related text including: portion, line, marks, classification, authority, banner, information, and placement.)



Three marking elements are required for classified NSI:

1. Portion marks
2. Banner line
3. Classification authority block

NOTE: Cover sheets may also be used to protect classified information from inadvertent disclosure and to alert observers that classified information is attached.

Select the next button for more information.

Anatomy of a Classified Document

Introduction

Three marking elements are required for classified NSI:

1. Portion marks
2. Banner line
3. Classification authority block

NOTE: Cover sheets may also be used to protect classified information from inadvertent disclosure and to alert observers that classified information is attached.

(Image alt: Mock up of a classified document that is marked with the appropriate classification, portion marks, and banner line.)

Portion Marks (Example 1)

"All documents containing information that requires control markings, regardless of classification, format, or medium, shall be portion marked."

~ ICD 710, Section D(5)

Portion marks reflect the highest classification level and most restrictive control markings of each portion. They appear in abbreviated form and are placed in parentheses at the beginning of all portions, immediately preceding the text to which they apply.

Portion marks must include the classification level, any necessary control markings, and shall be explicitly marked for appropriate foreign disclosure or release if classified.

This portion contains unclassified information.

(Image alt: An arrow animates to first portion mark on document)

Portion Marks (Example 2)
This portion mark includes SECRET (S) information with an SCI of Special Intelligence (SI) that is not releasable to foreign nationals (NF).

(Image alt: An arrow animates to second portion mark on document)

Banner Line
The banner line must be conspicuously placed at the top and bottom of each page in a way that distinguishes it from the informational text. The exterior or first page must include the highest classification and most restrictive control markings contained in the document. Each interior page of a classified document must have a banner line that contains **either** the highest classification and most restrictive control markings for information contained on that page **or** the highest classification and most restrictive control markings of the entire document.

NOTE: Classified documents shall be explicitly marked for appropriate foreign disclosure or release at the portion mark and banner line level in accordance with ICD 710.

(Image alt: An arrow animates to banner line in header of document)

Banner Line
The banner line must be conspicuously placed at the top and bottom of each page in a way that distinguishes it from the informational text.

(Image alt: Arrow animates to banner line in footer of document)

Classification Authority Block
The classification authority block must be placed on the front cover or the first page of a classified document.

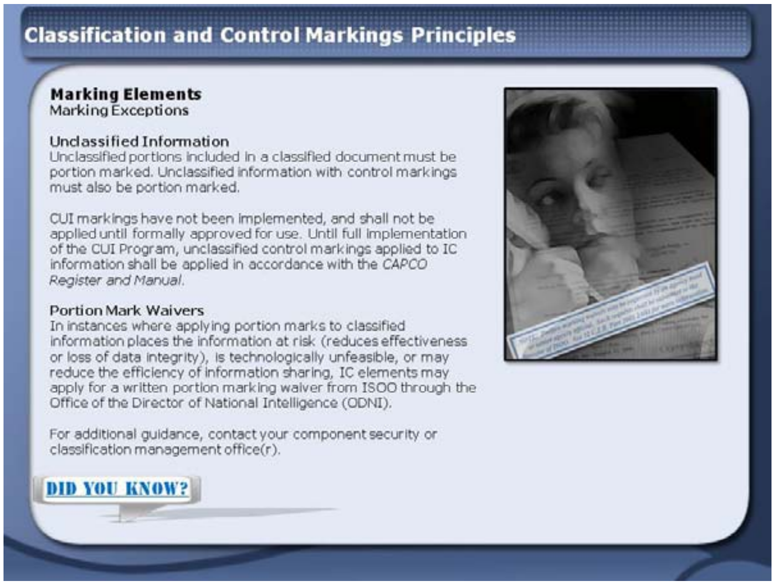
There are two forms of classification authority blocks:

- Original Classification Authority (OCA) block
- Derivative classification authority block

As a derivative classifier, your classification authority block will contain the following information:

- Classified By: (Name and position (or agency identification number) of person making classification decision)
- Derived From: (Authorized classification guide or derivative source document)
- Declassify On: (Declassification instructions from source or guide)

(Image alt: Arrow animates to classification authority block in document)



Classification and Control Markings Principles

Marking Elements
Marking Exceptions

Unclassified Information
Unclassified portions included in a classified document must be portion marked. Unclassified information with control markings must also be portion marked.

CUI markings have not been implemented, and shall not be applied until formally approved for use. Until full implementation of the CUI Program, unclassified control markings applied to IC information shall be applied in accordance with the *CAPCO Register and Manual*.

Portion Mark Waivers
In instances where applying portion marks to classified information places the information at risk (reduces effectiveness or loss of data integrity), is technologically unfeasible, or may reduce the efficiency of information sharing, IC elements may apply for a written portion marking waiver from ISOO through the Office of the Director of National Intelligence (ODNI).

For additional guidance, contact your component security or classification management office(r).

Marking Exceptions

Unclassified Information

Unclassified portions included in a classified document must be portion marked. Unclassified information with control markings must also be portion marked.

CUI markings have not been implemented, and shall not be applied until formally approved for use. Until full implementation of the CUI Program, unclassified control markings applied to IC information shall be applied in accordance with the *CAPCO Register and Manual*.

Portion Mark Waivers

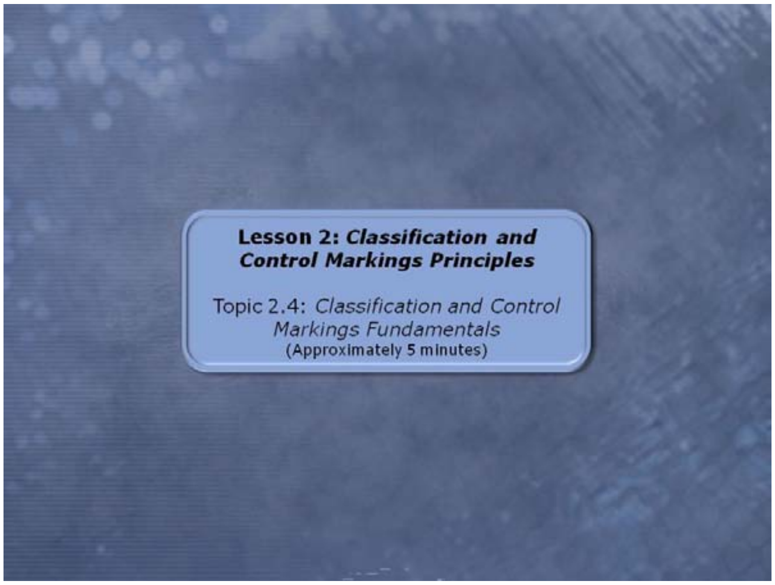
In instances where applying portion marks to classified information places the information at risk (reduces effectiveness or loss of data integrity), is technologically unfeasible, or may reduce the efficiency of information sharing, IC elements may apply for a written portion marking waiver from ISOO through the Office of the Director of National Intelligence (ODNI).

For additional guidance, contact your component security or classification management office(r).

Pop Up: Did You Know?

Any content in a document that is not portion marked cannot be used as a source for derivative classification.

(Image alt: Collage of a woman holding a feathered pen applying portion marks.)



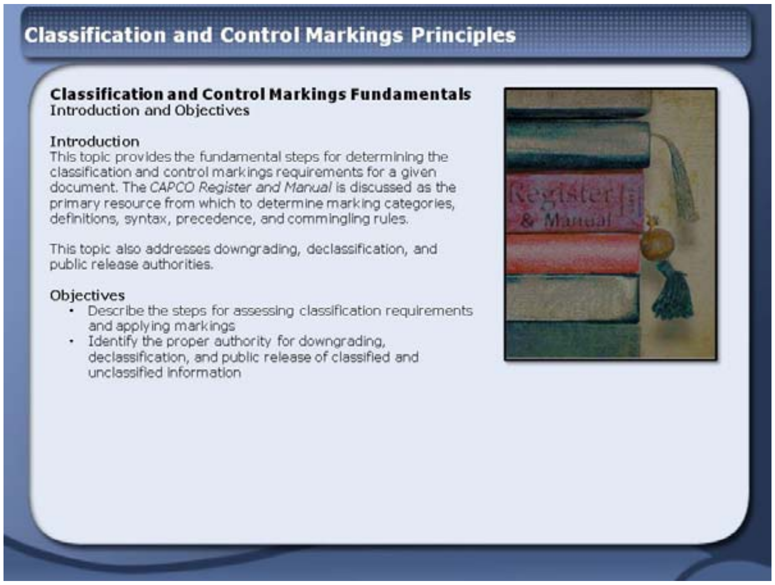
Lesson 2: *Classification and Control Markings Principles*

Topic 2.4: *Classification and Control Markings Fundamentals*
(Approximately 5 minutes)

Lesson 2: *Classification and Control Markings Principles*

Topic 2.4: *Classification and Control Markings Fundamentals*

(Approximately 5 minutes)



Classification and Control Markings Principles

Classification and Control Markings Fundamentals
Introduction and Objectives

Introduction
This topic provides the fundamental steps for determining the classification and control markings requirements for a given document. The *CAPCO Register and Manual* is discussed as the primary resource from which to determine marking categories, definitions, syntax, precedence, and commingling rules.

This topic also addresses downgrading, declassification, and public release authorities.

Objectives
- Describe the steps for assessing classification requirements and applying markings
- Identify the proper authority for downgrading, declassification, and public release of classified and unclassified information

Introduction and Objectives

Introduction

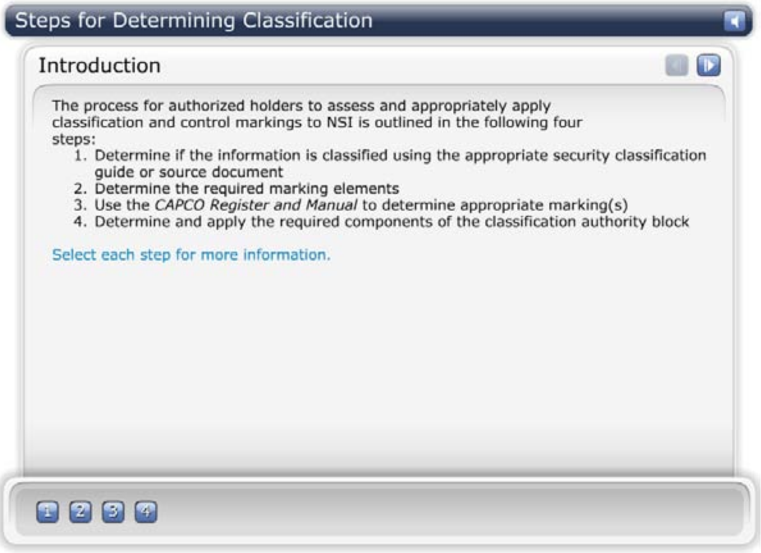
This topic provides the fundamental steps for determining the classification and control markings requirements for a given document. The *CAPCO Register and Manual* is discussed as the primary resource from which to determine marking categories, definitions, syntax, precedence, and commingling rules.

This topic also addresses downgrading, declassification, and public release authorities.

Objectives

- Describe the steps for assessing classification requirements and applying markings
- Identify the proper authority for downgrading, declassification, and public release of classified and unclassified information

(Image alt: A book labeled *Register & Manual*.)



Steps for Determining Classification

Introduction

The process for authorized holders to assess and appropriately apply classification and control markings to NSI is outlined in the following four steps:

1. Determine if the information is classified using the appropriate security classification guide or source document
2. Determine the required marking elements
3. Use the *CAPCO Register and Manual* to determine appropriate marking(s)
4. Determine and apply the required components of the classification authority block

Select each step for more information.

Steps for Determining Classification

Introduction

The process for authorized holders to assess and appropriately apply classification and control markings to NSI is outlined in the following four steps:

1. Determine if the information is classified using the appropriate security classification guide or source document
2. Determine the required marking elements
3. Use the *CAPCO Register and Manual* to determine appropriate marking(s)
4. Determine and apply the required components of the classification authority block

1. Classification Determination

Determine if the information is classified using the appropriate security classification guide or source document

NSI must meet the following three criteria to be classified:

- The information is owned by, produced by or for, or is under the control of the US Government
- The information meets one or more of the categories of information in Section 1.4 of EO 13526
- Unauthorized disclosure of the information reasonably could be expected to result in damage to the national security

Information that does not meet these criteria is not classified.

Authorized holders of classified NSI must use an authorized security classification guide(s) or a source document(s) to determine the appropriate classification level and control markings for a given portion or document. Individuals shall refer to the appropriate agency classification guide, relevant source document(s), or other form of OCA instruction for a classification determination.

For additional guidance, contact your component security or classification management office(r).

2. Required Marking Elements

Determine the required marking elements

Classified and controlled information require all three marking elements:

- Portion marks
- Banner line
- Classification authority block

Marking elements are not required for a wholly unclassified document. It is recommended, however, that unclassified documents in a classified environment should include a banner line to ensure that recipients understand how to protect the information and make informed decisions regarding dissemination and sharing. If unclassified information is transmitted over a classified system it must contain a banner line.

NOTE: Unclassified information contained in a classified document, must be portion marked to indicate appropriate handling and for further dissemination and sharing.

3. Marking Labels Application

Use the *CAPCO Register and Manual* to determine appropriate marking(s)

The *CAPCO Register and Manual* provides marking categories, definitions, syntax, precedence and commingling rules to assist authorized holders of NSI in applying markings for their classified and controlled documents.

Standard syntax enables computer systems to accurately route data and ensures effective information sharing, while withholding information from those not authorized to receive it.

Ensuring classified and controlled NSI is marked accurately allows authorized holders to make informed decisions regarding dissemination and sharing. Markings are a critical element of IC procedures for protecting classified information including intelligence sources and methods, while ensuring that information is available without delay or unnecessary restrictions.

4. Classification Authority Block Application

Determine and apply the required components of the classification authority block

There are three required elements of the classification authority block. The three elements vary depending on whether you are an OCA or a derivative classifier.

NOTE: When a document is classified derivatively on the basis of more than one source document or classification guide, the "Derived From" line shall contain "Multiple Sources," and a list of source materials must be included or attached to the derivatively classified document. In such cases, the "Declassify On" line will reflect the longest classification duration from among the sources listed on, or attached to, the classified document.

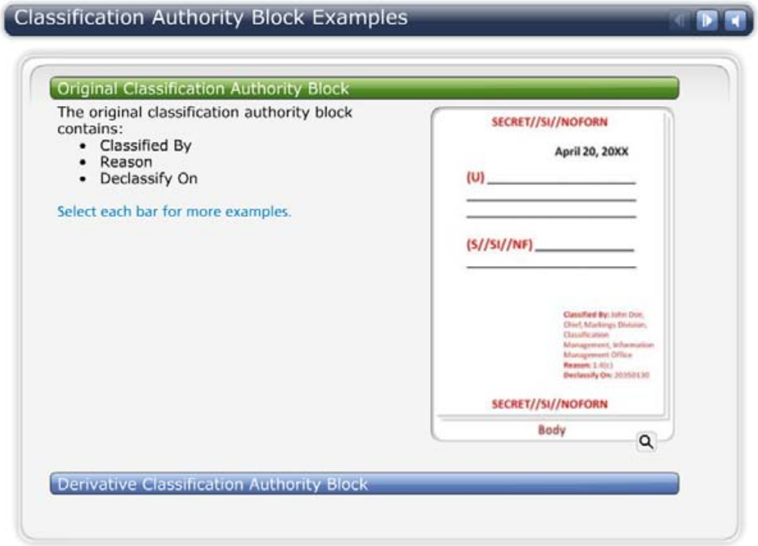
For additional guidance, contact your component security or classification management office(r).

Element	Derivative Classification Authority	Original Classification Authority
1	**Classified By:** The name and position (or agency identification number) of the person making the derivative classification determination	**Classified By:** The name and position (or personal identifier) of the OCA (and the agency and office of origin, if not otherwise evident)
2	**Derived From:** The source of the derivative classification determination (an authorized classification guide or source document)	**Reason:** The reason for classification (from classification categories provided in EO 13526, Section 1.4)
3	**Declassify On**: Declassification instructions, as directed by the authorized classification guide or source document. This is generally a	**Declassify On:** Declassification instructions. This is generally a date (YYYYMMDD), but may be an event, an exception, or other instructions

	date (YYYYMMDD), but may be an event, an exception, or other instructions	

Summary

Remember, as an authorized holder of classified NSI, you are responsible for protecting it from unauthorized disclosure, proper handling and safeguarding, and applying accurate classification and control markings.



Classification Authority Block Examples

Original Classification Authority Block

The original classification authority block contains:

- Classified By
- Reason
- Declassify On

Select each bar for more examples.

SECRET//SI//NOFORN

April 20, 20XX

(U)

(S//SI//NF)

Classified By: John Doe, Chief, Markings Division, Classification Management, Information Management Office
Reason: 1.4(c)
Declassify On: 20350130

SECRET//SI//NOFORN

Body

Derivative Classification Authority Block

Classification Authority Block Examples

Original Classification Authority Block

The original classification authority block contains:

- Classified By
- Reason
- Declassify On

(Image alt: Marked document with the following original classification authority block:

- **Classified By:** John Doe, Chief, Markings Division, Classification Management, Information Management Office
- **Reason:** 1.4(c)
- **Declassify On:** 20350130)

Derivative Classification Authority Block

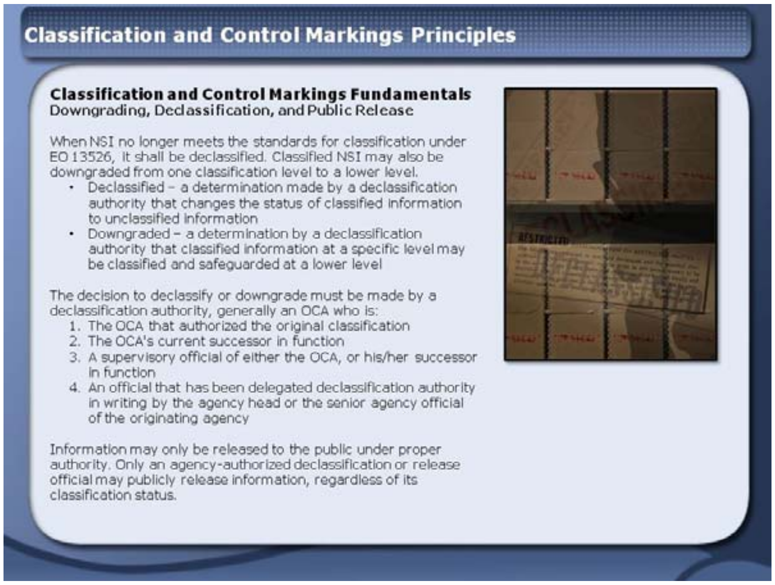
The derivative classification authority block contains:

- Classified By
- Derived From

- Declassify On

(Image alt: Marked document with the following derivative classification authority block:

- **Classified By:** John Doe/Analyst
- **Derived From:** Government Agency Security Classification Guide (SCG)
- **Declassify On:** 20350130)



Classification and Control Markings Principles

Classification and Control Markings Fundamentals
Downgrading, Declassification, and Public Release

When NSI no longer meets the standards for classification under EO 13526, it shall be declassified. Classified NSI may also be downgraded from one classification level to a lower level.

- Declassified – a determination made by a declassification authority that changes the status of classified information to unclassified information
- Downgraded – a determination by a declassification authority that classified information at a specific level may be classified and safeguarded at a lower level

The decision to declassify or downgrade must be made by a declassification authority, generally an OCA who is:

1. The OCA that authorized the original classification
2. The OCA's current successor in function
3. A supervisory official of either the OCA, or his/her successor in function
4. An official that has been delegated declassification authority in writing by the agency head or the senior agency official of the originating agency

Information may only be released to the public under proper authority. Only an agency-authorized declassification or release official may publicly release information, regardless of its classification status.

Downgrading, Declassification, and Public Release

When NSI no longer meets the standards for classification under EO 13526, it shall be declassified. Classified NSI may also be downgraded from one classification level to a lower level.

- Declassified – a determination made by a declassification authority that changes the status of classified information to unclassified information
- Downgraded – a determination by a declassification authority that classified information at a specific level may be classified and safeguarded at a lower level

The decision to declassify or downgrade must be made by a declassification authority, generally an OCA who is:

1. The OCA that authorized the original classification
2. The OCA's current successor in function
3. A supervisory official of either the OCA, or his/her successor in function
4. An official that has been delegated declassification authority in writing by the agency head or the senior agency official of the originating agency

Information may only be released to the public under proper authority. Only an agency-authorized declassification or release official may publicly release information, regardless of its classification status.

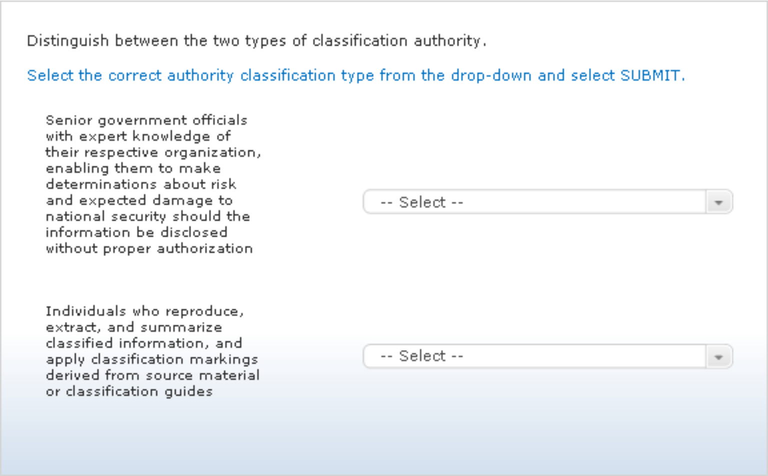
(Image alt: Image of classified NSI being marked DECLASSIFIED.)

Lesson 2 Knowledge Check

Introduction

The knowledge check consists of nine questions.
(Approximately 10 minutes)

NOTE: All examples are notional and are marked for training purposes only.



Distinguish between the two types of classification authority.

Select the correct authority classification type from the drop-down and select SUBMIT.

Senior government officials with expert knowledge of their respective organization, enabling them to make determinations about risk and expected damage to national security should the information be disclosed without proper authorization

Individuals who reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides

Topic 2.1

1 of 9: Distinguish between the two types of classification authority.

Select the correct authority classification type and continue reading for correct and incorrect feedback.

Definition	Authority Classification Types
Senior government officials with expert knowledge of their respective organization, enabling them to make determinations about risk and expected damage to national security should the information be disclosed without proper authorization	• Original Classification Authority (OCA) • Derivative Classification Authority
Individuals who reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides	• Original Classification Authority (OCA) • Derivative Classification Authority

The correct answers are:

- Original Classification Authority (OCA): Senior government officials with expert knowledge of their respective organization, enabling them to make determinations about risk and expected damage to national security should the information be disclosed without proper authorization
- Derivative Classification Authority: Individuals who reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides

Feedback when correct:
That's right! OCAs are senior government officials with expert knowledge of their respective organization, enabling them to make determinations about risk and expected damage to national security should the information be disclosed without proper authorization.

Derivative classifiers reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides.

Most authorized holders of classified National Security Information (NSI) are derivative classifiers.

Feedback when incorrect:
You did not select the correct responses.

OCAs are senior government officials with expert knowledge of their respective organization, enabling them to make determinations about risk and expected damage to national security should the information be disclosed without proper authorization.

Derivative classifiers reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides.

Most authorized holders of classified National Security Information (NSI) are derivative classifiers.

2 of 9: What resources are available to derivative classifiers as they determine and apply classification markings?

Select the correct response and continue reading for correct and incorrect feedback.

- Agency- or program-specific guides
- EO 13526
- ISOO Implementing Directive, 32 CFR Part 2001
- Component security or classification management office(r)
- All of the above

The correct answer is “All of the above.”

Feedback when correct:
That's right! When determining and applying classification markings, derivative classifiers should use all of the following resources:

- Agency- or program-specific guides
- EO 13526
- ISOO Implementing Directive, 32 CFR Part 2001
- Component security or classification management office(r)

Feedback when incorrect:
You did not select the correct response. The correct response is "All of the above."

When determining and applying classification markings, derivative classifiers should use all of the following resources:

- Agency- or program-specific guides
- EO 13526
- ISOO Implementing Directive, 32 CFR Part 2001
- Component security or classification management office(r)

Topic 2.2
3 of 9: Classified information is characterized by which of the following?

Select all that apply and continue reading for correct and incorrect feedback.

- The information requires protection against unauthorized disclosure and is marked to indicate its classified status
- The information is owned by, produced by or for, or is under the control of the US Government
- The information meets one or more of the categories of information in section 1.4 of EO 13526
- The OCA who classifies the information in the first instance, determines that unauthorized disclosure of the information reasonably could be expected to result in damage to the national security
- The information prevents embarrassment to a person, organization, or agency

The correct answers are:

- The information requires protection against unauthorized disclosure and is marked to indicate its classified status
- The information is owned by, produced by or for, or is under the control of the US Government
- The information meets one or more of the categories of information in section 1.4 of EO 13526
- The OCA who classifies the information in the first instance, determines that unauthorized disclosure of the information reasonably could be expected to result in damage to the national security

Feedback when correct:

That's right! EO 13526 defines classified information as information that requires protection against unauthorized disclosure and is marked to indicate its classified status.

Information may be classified if the following three criteria are met:

- The information is owned by, produced by or for, or is under the control of the US Government
- The information meets one or more of the categories of information in section 1.4 of EO 13526
- The OCA who classifies the information in the first instance, determines that unauthorized disclosure of the information reasonably could be expected to result in damage to the national security

Information shall not be classified in order to:

- Prevent embarrassment to a person, organization, or agency
- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of the national security

Feedback when incorrect:

You did not select the correct responses. The correct responses are:

- The information requires protection against unauthorized disclosure and is marked to indicate its classified status
- The information is owned by, produced by or for, or is under the control of the US Government

- The information meets one or more of the categories of information in section 1.4 of EO 13526
- The OCA who classifies the information in the first instance, determines that unauthorized disclosure of the information reasonably could be expected to result in damage to the national security

Information shall not be classified in order to:

- Prevent embarrassment to a person, organization, or agency
- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of the national security

4 of 9: Which of the following characterize control markings?

Select all that apply and continue reading for correct and incorrect information.

- Control markings can be applied to classified and unclassified information
- Control markings indicate additional safeguarding, handling, and/or dissemination requirements
- Guidance on appropriate application of control markings may be provided in individual agency classification guide(s)

The correct answers are:

- Control markings can be applied to classified and unclassified information
- Control markings indicate additional safeguarding, handling, and/or dissemination requirements
- Guidance on appropriate application of control markings may be provided in individual agency classification guide(s)

Feedback when correct:

That's right! All three of the following are characteristics of control markings:

- Control markings can be applied to classified and unclassified information
- Control markings indicate additional safeguarding, handling, and/or dissemination requirements
- Guidance on appropriate application of control markings may be provided in individual agency classification guide(s)

Feedback when incorrect:

You did not select the correct responses. The correct responses are:

- Control markings can be applied to classified and unclassified information
- Control markings indicate additional safeguarding, handling, and/or dissemination requirements
- Guidance on appropriate application of control markings may be provided in individual agency classification guide(s)

5 of 9: What is unclassified and Controlled Unclassified Information (CUI)?

Select the correct description for each term and continue reading for correct and incorrect feedback.

Terms	Descriptions
Unclassified information	• Information that does not meet the requirements for classification under EO 13526. • Unclassified information that requires additional control markings to indicate dissemination or distribution.
CUI	• Information that does not meet the requirements for classification under EO 13526. • Unclassified information that requires additional control markings to indicate dissemination or distribution.

The correct answers are:

- Unclassified information: Information that does not meet the requirements for classification under EO 13526.
- CUI: Unclassified information that requires additional control markings to indicate dissemination or distribution. These markings are still in development and shall not be applied until formally approved for use.

Feedback when correct:

That's right! Unclassified information does not meet the requirements for classification under EO 13526. CUI is unclassified information that requires additional control markings to indicate dissemination or distribution. These markings are still in development and shall not be applied until formally approved for use.

Feedback when incorrect:

You did not select the correct responses.

Unclassified information does not meet the requirements for classification under EO 13526. CUI is unclassified information that requires additional control markings to indicate dissemination or distribution. These markings are still in development and shall not be applied until formally approved for use.

Topic 2.3
6 of 9: What marking elements are required for classified information?

Select all that apply and continue reading for correct and incorrect feedback.

- Banner line
- Portion marks
- Classification authority block

The correct answers are:

- Banner line
- Portion marks
- Classification authority block

Feedback when correct:
That's right! All three of these marking elements are required for classified information. Completely unclassified information does not require any markings, but best practice is to apply a banner line. CUI requires portion marks and the banner line.

Feedback when incorrect:
You did not select the correct responses. The correct responses are:

- Portion marks
- Banner line
- Classification authority block

All three of these marking elements are required for classified information. Completely unclassified information does not require any markings, but best practice is to apply a banner line. CUI requires portion marks and the banner line.

7 of 9: Which of the following are instances in which portion marks are not required?

Select all that apply and continue reading for correct and incorrect feedback.

- When information is wholly unclassified
- When unclassified information is included in a classified document
- When a portion mark waiver has been approved for the information in question

The correct answers are:

- When information is wholly unclassified
- When a portion mark waiver has been approved for the information in question

Feedback when correct:
That's right! A document does not require marking elements when the information is wholly unclassified (though it is still good practice to do so) or when a portion mark waiver has been approved for the information in question. Unclassified information that is included in a classified document must be marked with "(U)."

Feedback when incorrect:
You did not select the correct responses. The correct responses are:

- When the information is wholly unclassified (though it is still good practice to do so)
- When a portion mark waiver has been approved for the information in question

Unclassified information that is included in a classified document must be marked with "(U)."

Topic 2.4

8 of 9: Put the four steps for assessing classification requirements and applying markings in order from step 1 through 4.

Place the steps in the proper order and continue reading for correct and incorrect feedback.

- Determine and apply the required components of the classification authority block
- Determine if the information is classified using the appropriate security classification guide or source document
- Determine the required marking elements
- Use the *CAPCO Register and Manual* to determine appropriate marking(s)

The correct order is:

1. Determine if the information is classified using the appropriate security classification guide or source document
2. Determine the required marking elements
3. Use the *CAPCO Register and Manual* to determine appropriate marking(s)
4. Determine and apply the required components of the classification authority block

Feedback when correct:

That's right! The four steps for assessing classification requirements and applying markings are:

1. Determine if the information is classified using the appropriate security classification guide or source document
2. Determine the required marking elements
3. Use the *CAPCO Register and Manual* to determine appropriate marking(s)
4. Determine and apply the required components of the classification authority block

Feedback when incorrect:

You did not select the correct response.

The four steps for assessing classification requirements and applying markings are:

1. Determine if the information is classified using the appropriate security classification guide or source document
2. Determine the required marking elements
3. Use the *CAPCO Register and Manual* to determine appropriate marking(s)
4. Determine and apply the required components of the classification authority block

9 of 9: The decision to declassify or downgrade must be made by a declassification authority, generally an Original Classification Authority (OCA).

Select True or False and continue reading for correct and incorrect feedback.

- True
- False

The correct answer is “True.”

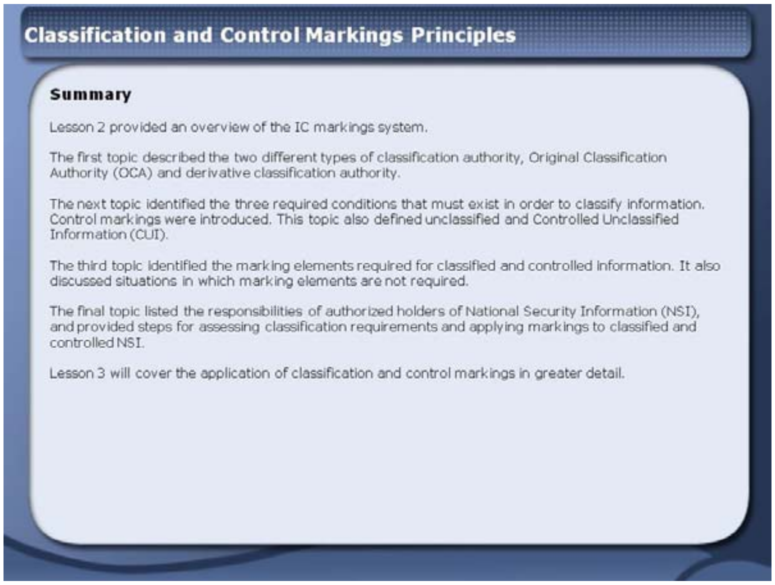
Feedback when correct:
That's right! The decision to declassify or downgrade must be made by a declassification authority, generally an Original Classification Authority (OCA) who is:

- The OCA that authorized the original classification
- The OCA's current successor in function
- A supervisory official of either the OCA, or his/her successor in function
- An official that has been delegated declassification authority in writing by the agency head or the senior agency official of the originating agency

Feedback when incorrect:
You did not select the correct response. The correct response is "True."

The decision to declassify or downgrade must be made by a declassification authority, generally an Original Classification Authority (OCA) who is:

- The OCA that authorized the original classification
- The OCA's current successor in function
- A supervisory official of either the OCA, or his/her successor in function
- An official that has been delegated declassification authority in writing by the agency head or the senior agency official of the originating agency



Classification and Control Markings Principles

Summary

Lesson 2 provided an overview of the IC markings system.

The first topic described the two different types of classification authority, Original Classification Authority (OCA) and derivative classification authority.

The next topic identified the three required conditions that must exist in order to classify information. Control markings were introduced. This topic also defined unclassified and Controlled Unclassified Information (CUI).

The third topic identified the marking elements required for classified and controlled information. It also discussed situations in which marking elements are not required.

The final topic listed the responsibilities of authorized holders of National Security Information (NSI), and provided steps for assessing classification requirements and applying markings to classified and controlled NSI.

Lesson 3 will cover the application of classification and control markings in greater detail.

Summary

Lesson 2 provided an overview of the IC markings system.

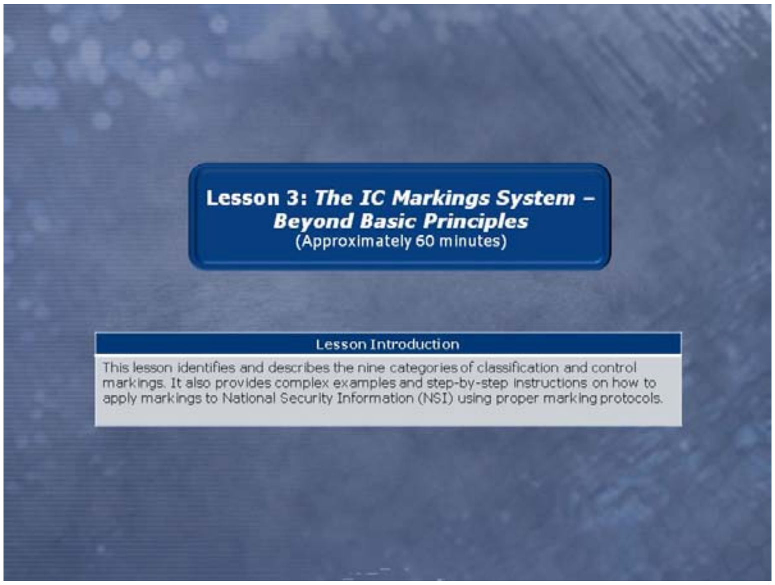
The first topic described the two different types of classification authority, Original Classification Authority (OCA) and derivative classification authority.

The next topic identified the three required conditions that must exist in order to classify information. Control markings were introduced. This topic also defined unclassified and Controlled Unclassified Information (CUI).

The third topic identified the marking elements required for classified and controlled information. It also discussed situations in which marking elements are not required.

The final topic listed the responsibilities of authorized holders of National Security Information (NSI), and provided steps for assessing classification requirements and applying markings to classified and controlled NSI.

Lesson 3 will cover the application of classification and control markings in greater detail.


Lesson 3: *The IC Markings System – Beyond Basic Principles*
(Approximately 60 minutes)

Lesson Introduction

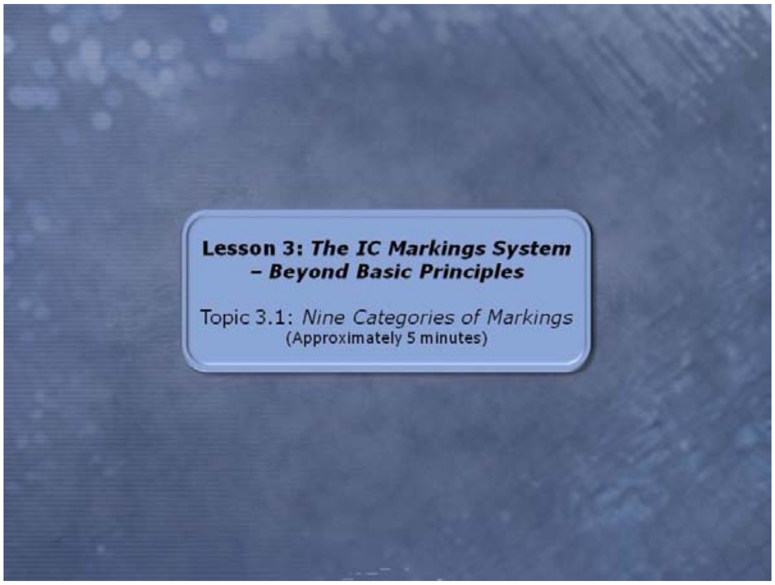
This lesson identifies and describes the nine categories of classification and control markings. It also provides complex examples and step-by-step instructions on how to apply markings to National Security Information (NSI) using proper marking protocols.

Lesson 3: *The IC Markings System – Beyond Basic Principles*

(Approximately 60 minutes)

Lesson Introduction

This lesson identifies and describes the nine categories of classification and control markings. It also provides complex examples and step-by-step instructions on how to apply markings to National Security Information (NSI) using proper marking protocols.

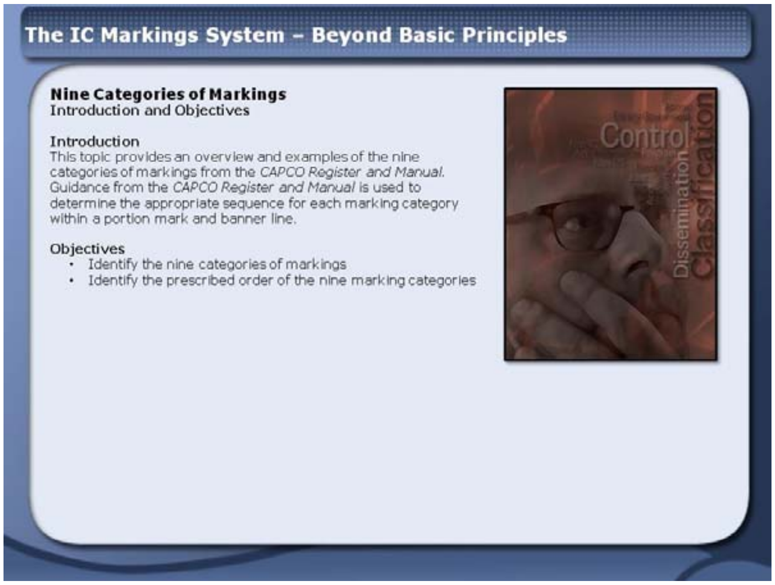

Lesson 3: *The IC Markings System – Beyond Basic Principles*

Topic 3.1: *Nine Categories of Markings*
(Approximately 5 minutes)

Lesson 3: *The IC Marking System – Beyond Basic Principles*

Topic 3.1: *Nine Categories of Markings*

(Approximately 5 minutes)



The IC Markings System – Beyond Basic Principles

Nine Categories of Markings
Introduction and Objectives

Introduction
This topic provides an overview and examples of the nine categories of markings from the *CAPCO Register and Manual.* Guidance from the *CAPCO Register and Manual* is used to determine the appropriate sequence for each marking category within a portion mark and banner line.

Objectives

- Identify the nine categories of markings
- Identify the prescribed order of the nine marking categories

Introduction and Objectives

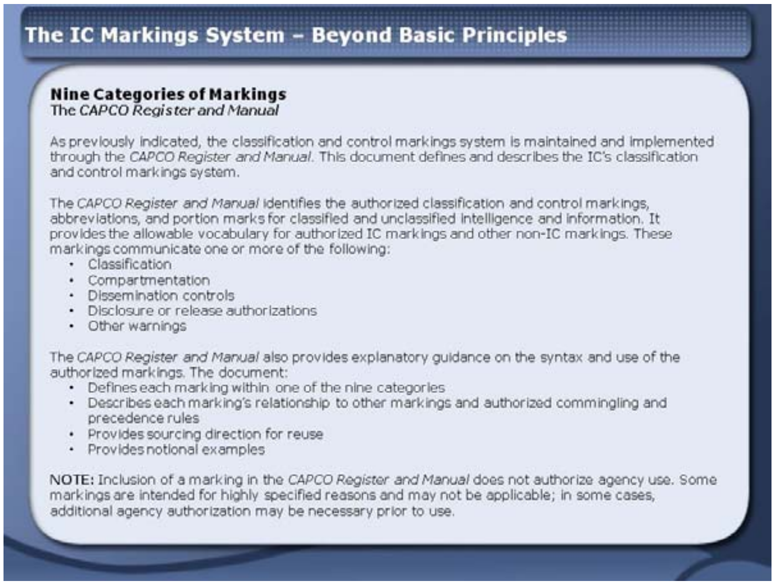
Introduction

This topic provides an overview and examples of the nine categories of markings from the *CAPCO Register and Manual*. Guidance from the *CAPCO Register and Manual* is used to determine the appropriate sequence for each marking category within a portion mark and banner line.

Objectives

- Identify the nine categories of markings
- Identify the prescribed order of the nine marking categories

(Image alt: Image of a man identifying the marking category with text: control, dissemination, classification.)



The IC Markings System – Beyond Basic Principles

Nine Categories of Markings
The CAPCO Register and Manual

As previously indicated, the classification and control markings system is maintained and implemented through the *CAPCO Register and Manual*. This document defines and describes the IC's classification and control markings system.

The *CAPCO Register and Manual* identifies the authorized classification and control markings, abbreviations, and portion marks for classified and unclassified intelligence and information. It provides the allowable vocabulary for authorized IC markings and other non-IC markings. These markings communicate one or more of the following:

- Classification
- Compartmentation
- Dissemination controls
- Disclosure or release authorizations
- Other warnings

The *CAPCO Register and Manual* also provides explanatory guidance on the syntax and use of the authorized markings. The document:

- Defines each marking within one of the nine categories
- Describes each marking's relationship to other markings and authorized commingling and precedence rules
- Provides sourcing direction for reuse
- Provides notional examples

NOTE: Inclusion of a marking in the *CAPCO Register and Manual* does not authorize agency use. Some markings are intended for highly specified reasons and may not be applicable; in some cases, additional agency authorization may be necessary prior to use.

The *CAPCO Register and Manual*

As previously indicated, the classification and control markings system is maintained and implemented through the *CAPCO Register and Manual*. This document defines and describes the IC's classification and control markings system.

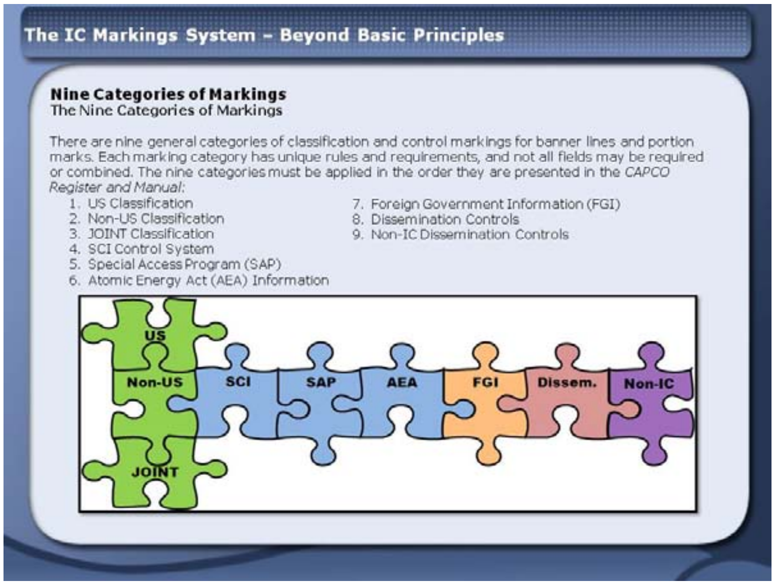
The *CAPCO Register and Manual* identifies the authorized classification and control markings, abbreviations, and portion marks for classified and unclassified intelligence and information. It provides the allowable vocabulary for authorized IC markings and other non-IC markings. These markings communicate one or more of the following:

- Classification
- Compartmentation
- Dissemination controls
- Disclosure or release authorizations
- Other warnings

The *CAPCO Register and Manual* also provides explanatory guidance on the syntax and use of the authorized markings. The document:

- Defines each marking within one of the nine categories
- Describes each marking's relationship to other markings and authorized commingling and precedence rules
- Provides sourcing direction for reuse
- Provides notional examples

NOTE: Inclusion of a marking in the *CAPCO Register and Manual* does not authorize agency use. Some markings are intended for highly specified reasons and may not be applicable; in some cases, additional agency authorization may be necessary prior to use.



The IC Markings System – Beyond Basic Principles

Nine Categories of Markings
The Nine Categories of Markings

There are nine general categories of classification and control markings for banner lines and portion marks. Each marking category has unique rules and requirements, and not all fields may be required or combined. The nine categories must be applied in the order they are presented in the *CAPCO Register and Manual:*

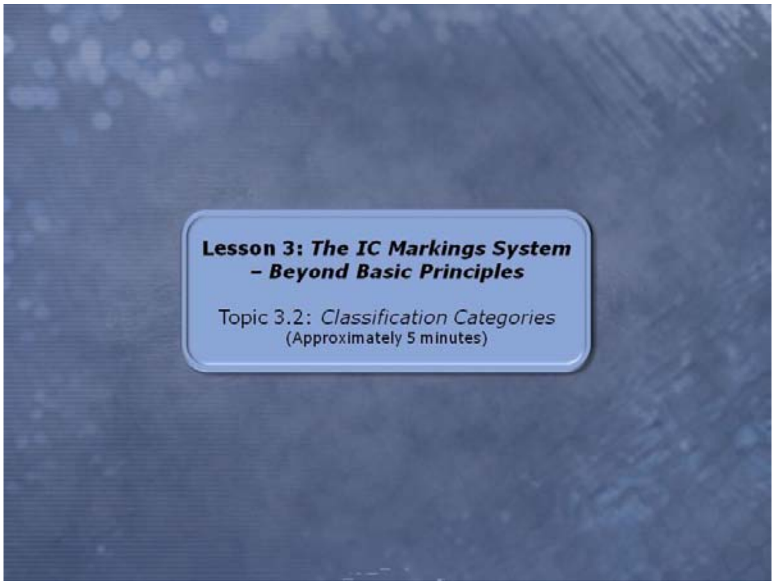
1. US Classification
2. Non-US Classification
3. JOINT Classification
4. SCI Control System
5. Special Access Program (SAP)
6. Atomic Energy Act (AEA) Information
7. Foreign Government Information (FGI)
8. Dissemination Controls
9. Non-IC Dissemination Controls

The Nine Categories of Markings

There are nine general categories of classification and control markings for banner lines and portion marks. Each marking category has unique rules and requirements, and not all fields may be required or combined. The nine categories must be applied in the order they are presented in the *CAPCO Register and Manual*:

1. US Classification
2. Non-US Classification
3. JOINT Classification
4. SCI Control System
5. Special Access Program (SAP)
6. Atomic Energy Act (AEA) Information
7. Foreign Government Information (FGI)
8. Dissemination Controls
9. Non-IC Dissemination Controls

(Image alt: Puzzle pieces with the nine categories of markings: US, Non-US, JOINT, SCI, SAP, AEA, FGI, Dissem., and Non-IC.)



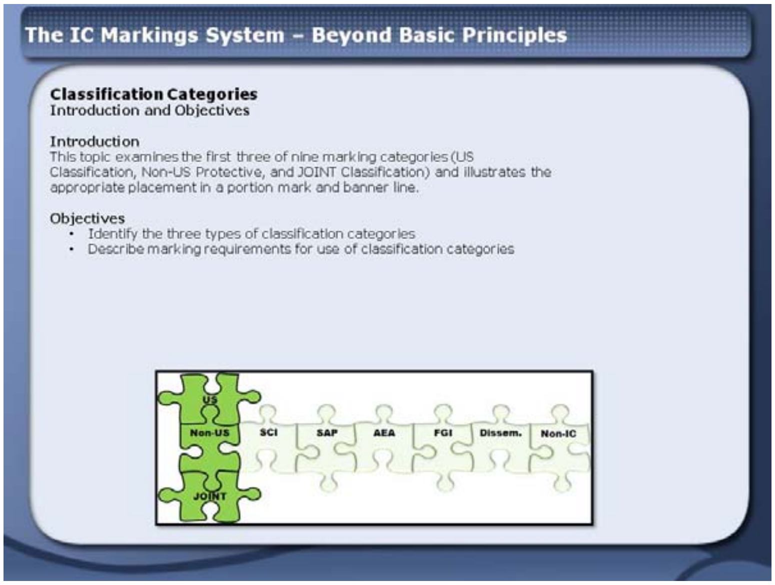
Lesson 3: *The IC Markings System – Beyond Basic Principles*

Topic 3.2: *Classification Categories*
(Approximately 5 minutes)

Lesson 3: *The IC Marking System – Beyond Basic Principles*

Topic 3.2: *Classification Categories*

(Approximately 5 minutes)



The IC Markings System – Beyond Basic Principles

Classification Categories
Introduction and Objectives

Introduction
This topic examines the first three of nine marking categories (US Classification, Non-US Protective, and JOINT Classification) and illustrates the appropriate placement in a portion mark and banner line.

Objectives
- Identify the three types of classification categories
- Describe marking requirements for use of classification categories

Introduction and Objectives

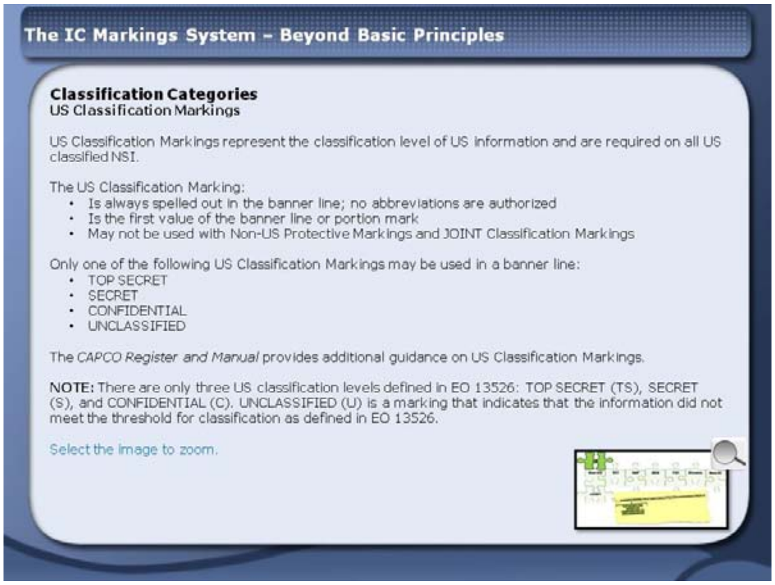
Introduction

This topic examines the first three of nine marking categories (US Classification, Non-US Protective, and JOINT Classification) and illustrates the appropriate placement in a portion mark and banner line.

Objectives

- Identify the three types of classification categories
- Describe marking requirements for use of classification categories

(Image alt: Puzzle pieces showing each of the nine categories of markings with the US, Non-US, and JOINT pieces highlighted.)



The IC Markings System – Beyond Basic Principles

Classification Categories
US Classification Markings

US Classification Markings represent the classification level of US information and are required on all US classified NSI.

The US Classification Marking:

- Is always spelled out in the banner line; no abbreviations are authorized
- Is the first value of the banner line or portion mark
- May not be used with Non-US Protective Markings and JOINT Classification Markings

Only one of the following US Classification Markings may be used in a banner line:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- UNCLASSIFIED

The *CAPCO Register and Manual* provides additional guidance on US Classification Markings.

NOTE: There are only three US classification levels defined in EO 13526: TOP SECRET (TS), SECRET (S), and CONFIDENTIAL (C). UNCLASSIFIED (U) is a marking that indicates that the information did not meet the threshold for classification as defined in EO 13526.

Select the image to zoom.

US Classification Markings

US Classification Markings represent the classification level of US information and are required on all US classified NSI.

The US Classification Marking:

- Is always spelled out in the banner line; no abbreviations are authorized
- Is the first value of the banner line or portion mark
- May not be used with Non-US Protective Markings and JOINT Classification Markings

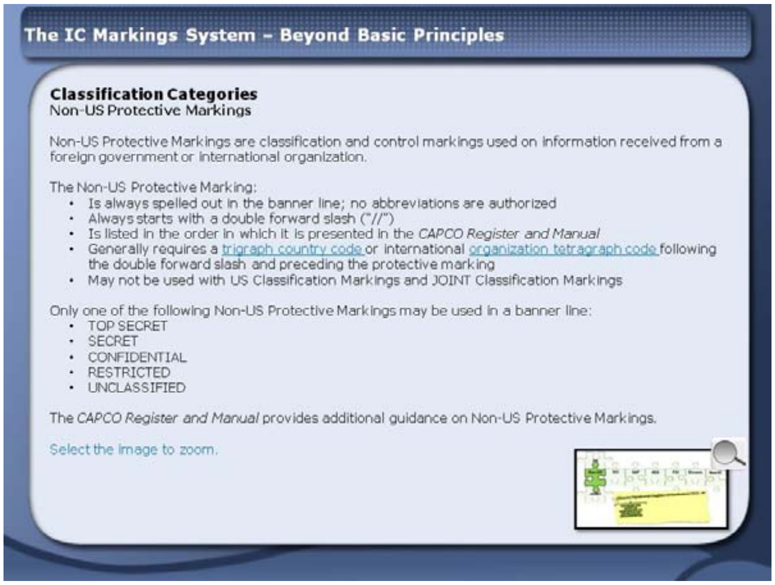
Only one of the following US Classification Markings may be used in a banner line:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- UNCLASSIFIED

The *CAPCO Register and Manual* provides additional guidance on US Classification Markings.

NOTE: There are only three US classification levels defined in EO 13526: TOP SECRET (TS), SECRET (S), and CONFIDENTIAL (C). UNCLASSIFIED (U) is a marking that indicates that the information did not meet the threshold for classification as defined in EO 13526.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the US piece highlighted. An example banner line highlights CLASSIFICATION with additional information: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), UNCLASSIFIED (U).)



The IC Markings System – Beyond Basic Principles

Classification Categories
Non-US Protective Markings

Non-US Protective Markings are classification and control markings used on information received from a foreign government or international organization.

The Non-US Protective Marking:

- Is always spelled out in the banner line; no abbreviations are authorized
- Always starts with a double forward slash ("//")
- Is listed in the order in which it is presented in the *CAPCO Register and Manual*
- Generally requires a trigraph country code or international organization tetragraph code following the double forward slash and preceding the protective marking
- May not be used with US Classification Markings and JOINT Classification Markings

Only one of the following Non-US Protective Markings may be used in a banner line:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED
- UNCLASSIFIED

The *CAPCO Register and Manual* provides additional guidance on Non-US Protective Markings.

Select the image to zoom.

Non-US Protective Markings

Non-US Protective Markings are classification and control markings used on information received from a foreign government or international organization.

The Non-US Protective Marking:

- Is always spelled out in the banner line; no abbreviations are authorized
- Always starts with a double forward slash ("//")
- Is listed in the order in which it is presented in the *CAPCO Register and Manual*
- Generally requires a trigraph country code or international organization tetragraph code following the double forward slash and preceding the protective marking
- May not be used with US Classification Markings and JOINT Classification Markings

Only one of the following Non-US Protective Markings may be used in a banner line:

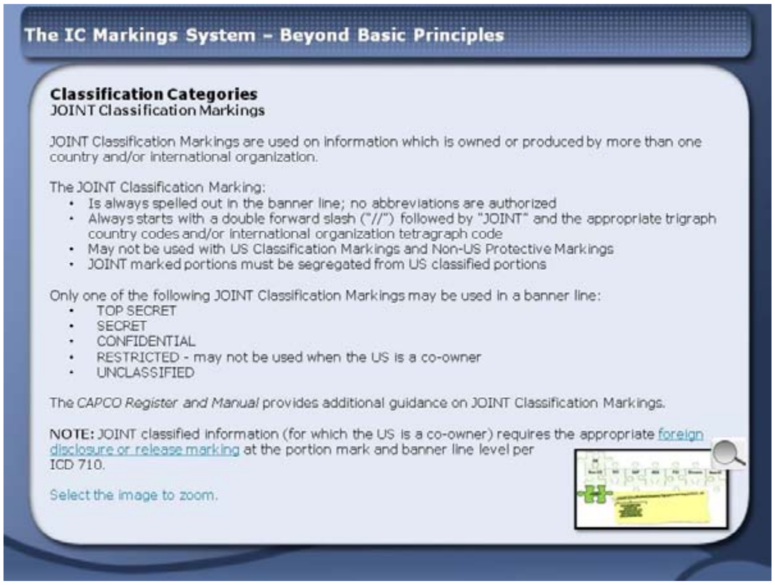
- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED
- UNCLASSIFIED

The *CAPCO Register and Manual* provides additional guidance on Non-US Protective Markings.

Pop Up: Trigraph Country Code
A trigraph country code is a three-letter country code used to represent a country (or countries) for purposes of disclosure, release, or indicators of FGI. Trigraphs are authorized for use in accordance with applicable US foreign sharing guidance or Concept of Operations (CONOP). The International Standards Organization (ISO) maintains the standard for trigraphs in the ISO 3166.

Pop Up: Organization Tetragraph Code
Organization tetragraph codes are four-character codes used to represent international organizations, coalitions, and alliances for purposes of disclosure, release, or indicators of FGI. Tetragraphs are authorized for use in accordance with applicable US foreign sharing guidance or CONOPs. CAPCO maintains the list of authorized tetragraph codes in the *CAPCO Register and Manual, Annex B*.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Non-US piece highlighted. An example banner line highlights //[Country Trigraph or Int'l Org][Non-US Classification] with additional information: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), RESTRICTED (R), UNCLASSIFIED (U).)



The IC Markings System – Beyond Basic Principles

Classification Categories
JOINT Classification Markings

JOINT Classification Markings are used on information which is owned or produced by more than one country and/or international organization.

The JOINT Classification Marking:

- Is always spelled out in the banner line; no abbreviations are authorized
- Always starts with a double forward slash ("//") followed by "JOINT" and the appropriate trigraph country codes and/or international organization tetragraph code
- May not be used with US Classification Markings and Non-US Protective Markings
- JOINT marked portions must be segregated from US classified portions

Only one of the following JOINT Classification Markings may be used in a banner line:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED - may not be used when the US is a co-owner
- UNCLASSIFIED

The *CAPCO Register and Manual* provides additional guidance on JOINT Classification Markings.

NOTE: JOINT classified information (for which the US is a co-owner) requires the appropriate foreign disclosure or release marking at the portion mark and banner line level per ICD 710.

Select the image to zoom.

JOINT Classification Markings

JOINT Classification Markings are used on information which is owned or produced by more than one country and/or international organization.

The JOINT Classification Marking:

- Is always spelled out in the banner line; no abbreviations are authorized
- Always starts with a double forward slash ("//") followed by "JOINT" and the appropriate trigraph country codes and/or international organization tetragraph code
- May not be used with US Classification Markings and Non-US Protective Markings
- JOINT marked portions must be segregated from US classified portions

Only one of the following JOINT Classification Markings may be used in a banner line:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED - may not be used when the US is a co-owner
- UNCLASSIFIED

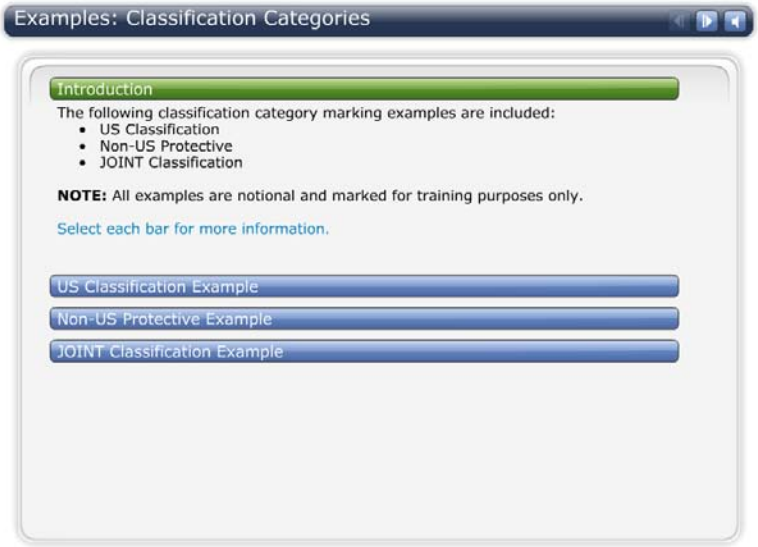
The *CAPCO Register and Manual* provides additional guidance on JOINT Classification Markings.

NOTE: JOINT classified information (for which the US is a co-owner) requires the appropriate foreign disclosure or release marking at the portion mark and banner line level per ICD 710.

Pop Up: Foreign Disclosure or Release Marking

Foreign disclosure or release marking are applied to classified intelligence to communicate the type of foreign disclosure or release decision. For additional implementation guidance, see the *CAPCO Manual*.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the JOINT piece highlighted. An example banner line highlights //JOINT [Classification] [Country Trigraph or Int'l Org] with additional information: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), RESTRICTED (R), UNCLASSIFIED (U).



Examples: Classification Categories

Introduction

The following classification category marking examples are included:

- US Classification
- Non-US Protective
- JOINT Classification

NOTE: All examples are notional and marked for training purposes only.

Select each bar for more information.

US Classification Example
Non-US Protective Example
JOINT Classification Example

Examples: Classification Categories

Introduction

The following classification category marking examples are included:

- US Classification
- Non-US Protective
- JOINT Classification

NOTE: All examples are notional and marked for training purposes only.

US Classification Example

TOP SECRET//NOFORN

(TS//NF) This portion is classified TOP SECRET (TS) and is not releasable to foreign nationals (NOFORN (NF)).

(S//NF) This portion is classified SECRET (S) and is not releasable to foreign nationals (NOFORN (NF)).

(U) **NOTE:** As defined by and under the purview of ICD 710, classified information shall be explicitly marked for appropriate foreign disclosure or release at the portion mark and banner line level. Originators of intelligence information are responsible for determining and appropriately applying classification and dissemination control markings (foreign and domestic) for the information they produce. “NOFORN” is a foreign release marking and is used in this example.

Classify By: __________
Derived From: ______
Declassify On: _______

TOP SECRET//NOFORN

Non-US Protective Example

//DEU SECRET

(//DEU S) This portion is classified German (DEU) SECRET (S). Use ISO 3166 trigraph country code or international organization tetragraph code to represent non-US classified material.

(U) **NOTE:** All non-US classified material is exempt from EO 13526 marking requirements. Therefore, non-US classified material does not carry a classification authority block.

//DEU SECRET

JOINT Classification Example

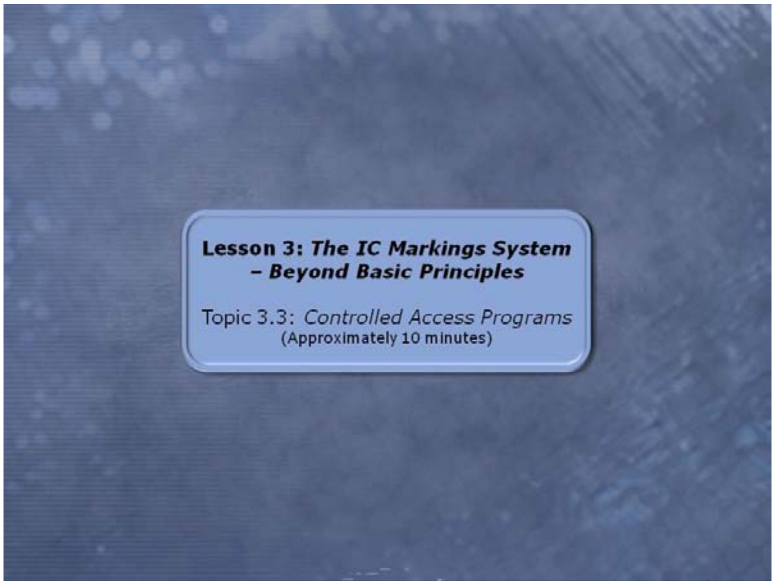
//JOINT SECRET CAN GBR USA//REL TO USA, CAN, GBR

(//JOINT S//REL TO USA, CAN, GBR) This portion is classified JOINT Canada (CAN), United Kingdom (GBR), and United States (USA) SECRET (S). The JOINT portion mark indicates co-ownership and releasability (REL TO) of the entire portion only to the co-owners (USA, CAN, GBR).

(U) **NOTE:** All JOINT information is withheld from further release until approved for release by the co-owners.

(U) **NOTE:** The classification authority block is required on all JOINT classified information in which the US is one of the co-owners. See the ISOO Implementing Directive and General Marking Guidance Section of the *CAPCO Manual* for more information.

Classify By: __________
Derived From: ______
Declassify On: _______



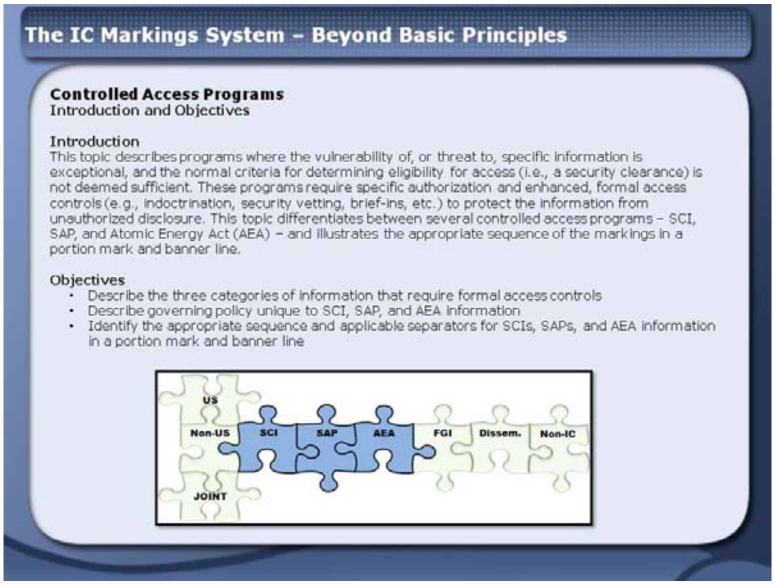
Lesson 3: *The IC Markings System – Beyond Basic Principles*

Topic 3.3: *Controlled Access Programs*
(Approximately 10 minutes)

Lesson 3: *The IC Marking System – Beyond Basic Principles*

Topic 3.3: *Controlled Access Programs*

(Approximately 10 minutes)



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
Introduction and Objectives

Introduction
This topic describes programs where the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access (i.e., a security clearance) is not deemed sufficient. These programs require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure. This topic differentiates between several controlled access programs – SCI, SAP, and Atomic Energy Act (AEA) – and illustrates the appropriate sequence of the markings in a portion mark and banner line.

Objectives
- Describe the three categories of information that require formal access controls
- Describe governing policy unique to SCI, SAP, and AEA information
- Identify the appropriate sequence and applicable separators for SCIs, SAPs, and AEA information in a portion mark and banner line

Introduction and Objectives

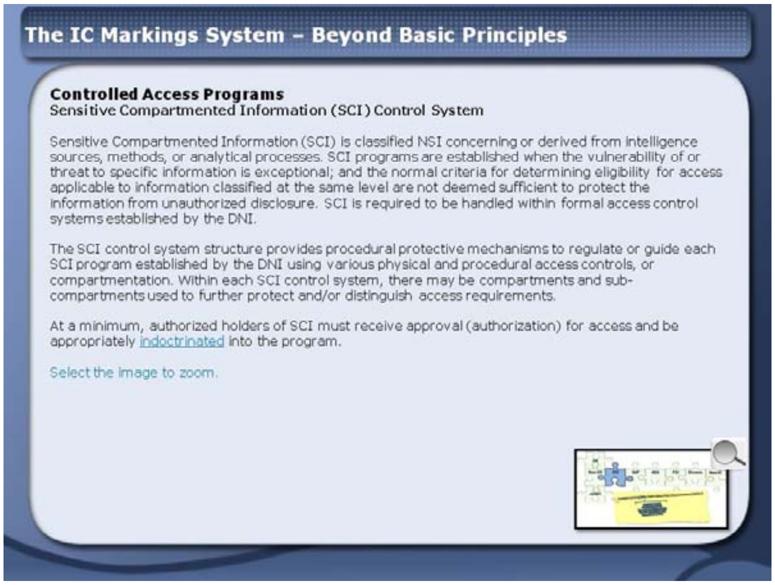
Introduction

This topic describes programs where the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access (i.e., a security clearance) is not deemed sufficient. These programs require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure. This topic differentiates between several controlled access programs – SCI, SAP, and Atomic Energy Act (AEA) – and illustrates the appropriate sequence of the markings in a portion mark and banner line.

Objectives

- Describe the three categories of information that require formal access controls
- Describe governing policy unique to SCI, SAP, and AEA information
- Identify the appropriate sequence and applicable separators for SCIs, SAPs, and AEA information in a portion mark and banner line

(Image alt: Puzzle pieces showing each of the nine categories of markings with the SCI, SAP, and AEA pieces highlighted.)



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
Sensitive Compartmented Information (SCI) Control System

Sensitive Compartmented Information (SCI) is classified NSI concerning or derived from intelligence sources, methods, or analytical processes. SCI programs are established when the vulnerability of or threat to specific information is exceptional; and the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure. SCI is required to be handled within formal access control systems established by the DNI.

The SCI control system structure provides procedural protective mechanisms to regulate or guide each SCI program established by the DNI using various physical and procedural access controls, or compartmentation. Within each SCI control system, there may be compartments and sub-compartments used to further protect and/or distinguish access requirements.

At a minimum, authorized holders of SCI must receive approval (authorization) for access and be appropriately indoctrinated into the program.

Select the image to zoom.

Sensitive Compartmented Information (SCI) Control System

Sensitive Compartmented Information (SCI) is classified NSI concerning or derived from intelligence sources, methods, or analytical processes. SCI programs are established when the vulnerability of or threat to specific information is exceptional; and the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure. SCI is required to be handled within formal access control systems established by the DNI.

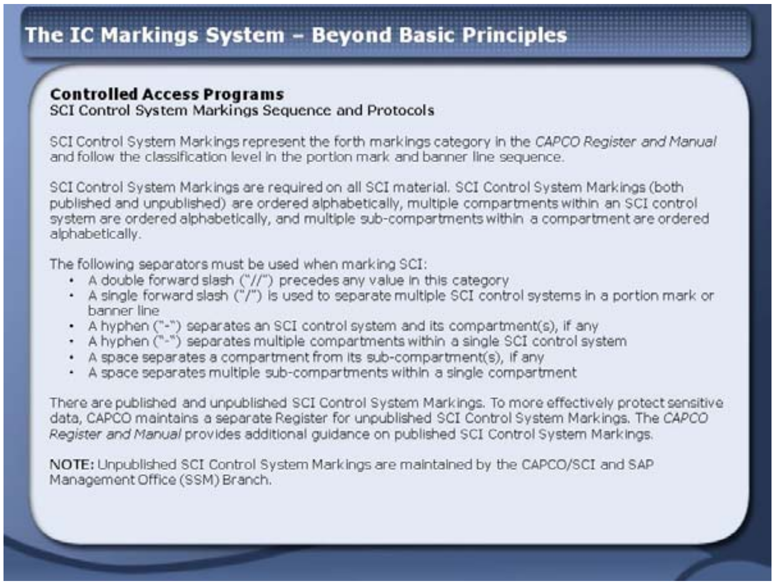
The SCI control system structure provides procedural protective mechanisms to regulate or guide each SCI program established by the DNI using various physical and procedural access controls, or compartmentation. Within each SCI control system, there may be compartments and sub-compartments used to further protect and/or distinguish access requirements.

At a minimum, authorized holders of SCI must receive approval (authorization) for access and be appropriately indoctrinated into the program.

Pop Up: Indoctrinated

The indoctrination process also informs the recipient of the sensitivity of the information and appropriate cautions concerning answers to questions from non-briefed persons, such as family, personal associates, media, and journalists.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the SCI piece highlighted. An example banner line highlights //SCI with additional information: HUMINT (HCS), KLONDIKE (KDK), Special Intelligence (SI), TALENT KEYHOLE (TK), Unpublished SCIs.)



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
SCI Control System Markings Sequence and Protocols

SCI Control System Markings represent the forth markings category in the *CAPCO Register and Manual* and follow the classification level in the portion mark and banner line sequence.

SCI Control System Markings are required on all SCI material. SCI Control System Markings (both published and unpublished) are ordered alphabetically, multiple compartments within an SCI control system are ordered alphabetically, and multiple sub-compartments within a compartment are ordered alphabetically.

The following separators must be used when marking SCI:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") is used to separate multiple SCI control systems in a portion mark or banner line
- A hyphen ("-") separates an SCI control system and its compartment(s), if any
- A hyphen ("-") separates multiple compartments within a single SCI control system
- A space separates a compartment from its sub-compartment(s), if any
- A space separates multiple sub-compartments within a single compartment

There are published and unpublished SCI Control System Markings. To more effectively protect sensitive data, CAPCO maintains a separate Register for unpublished SCI Control System Markings. The *CAPCO Register and Manual* provides additional guidance on published SCI Control System Markings.

NOTE: Unpublished SCI Control System Markings are maintained by the CAPCO/SCI and SAP Management Office (SSM) Branch.

SCI Control System Markings Sequence and Protocols

SCI Control System Markings represent the fourth markings category in the *CAPCO Register and Manual* and follow the classification level in the portion mark and banner line sequence.

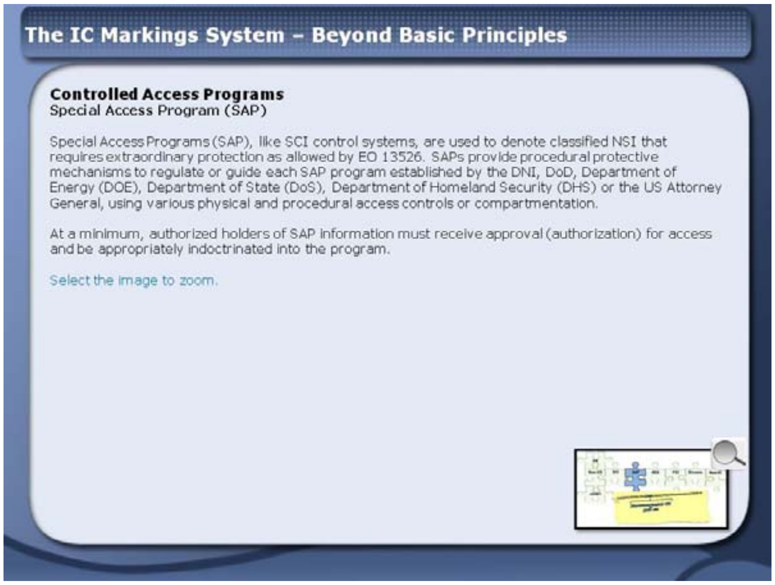
SCI Control System Markings are required on all SCI material. SCI Control System Markings (both published and unpublished) are ordered alphabetically, multiple compartments within an SCI control system are ordered alphabetically, and multiple sub-compartments within a compartment are ordered alphabetically.

The following separators must be used when marking SCI:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") is used to separate multiple SCI control systems in a portion mark or banner line
- A hyphen ("-") separates an SCI control system and its compartment(s), if any
- A hyphen ("-") separates multiple compartments within a single SCI control system
- A space separates a compartment from its sub-compartment(s), if any
- A space separates multiple sub-compartments within a single compartment

There are published and unpublished SCI Control System Markings. To more effectively protect sensitive data, CAPCO maintains a separate Register for unpublished SCI Control System Markings. The *CAPCO Register and Manual* provides additional guidance on published SCI control markings.

NOTE: Unpublished SCI Control System Markings are maintained by the CAPCO/SCI and SAP Management Office (SSM) Branch.



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
Special Access Program (SAP)

Special Access Programs (SAP), like SCI control systems, are used to denote classified NSI that requires extraordinary protection as allowed by EO 13526. SAPs provide procedural protective mechanisms to regulate or guide each SAP program established by the DNI, DoD, Department of Energy (DOE), Department of State (DoS), Department of Homeland Security (DHS) or the US Attorney General, using various physical and procedural access controls or compartmentation.

At a minimum, authorized holders of SAP information must receive approval (authorization) for access and be appropriately indoctrinated into the program.

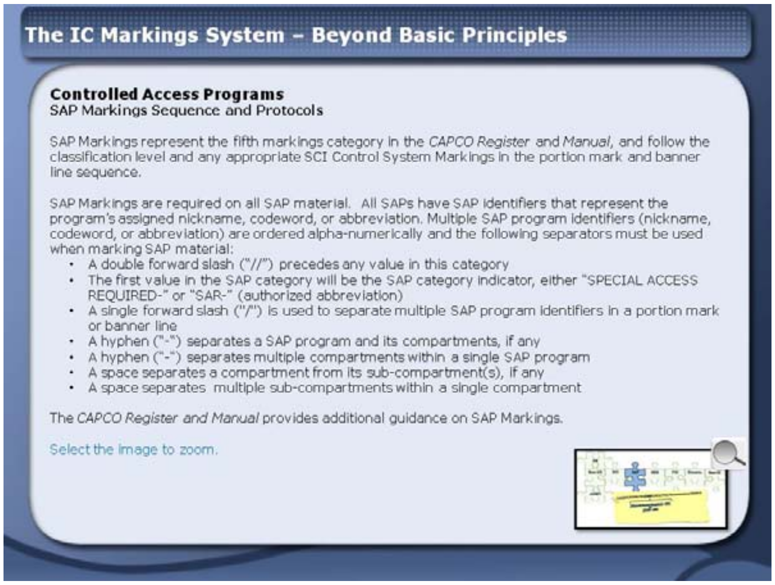
Select the image to zoom.

Special Access Program (SAP)

Special Access Programs (SAP), like SCI control systems, are used to denote classified NSI that requires extraordinary protection as allowed by EO 13526. SAPs provide procedural protective mechanisms to regulate or guide each SAP program established by the DNI, DoD, Department of Energy (DOE), Department of State (DoS), Department of Homeland Security (DHS) or the US Attorney General, using various physical and procedural access controls or compartmentation.

At a minimum, authorized holders of SAP information must receive approval (authorization) for access and be appropriately indoctrinated into the program.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the SAP piece highlighted. An example banner line highlights //SAP with additional information: //Special Access Required-ABC or //SAR-ABC.)



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
SAP Markings Sequence and Protocols

SAP Markings represent the fifth markings category in the *CAPCO Register* and *Manual*, and follow the classification level and any appropriate SCI Control System Markings in the portion mark and banner line sequence.

SAP Markings are required on all SAP material. All SAPs have SAP identifiers that represent the program's assigned nickname, codeword, or abbreviation. Multiple SAP program identifiers (nickname, codeword, or abbreviation) are ordered alpha-numerically and the following separators must be used when marking SAP material:

- A double forward slash ("//") precedes any value in this category
- The first value in the SAP category will be the SAP category indicator, either "SPECIAL ACCESS REQUIRED-" or "SAR-" (authorized abbreviation)
- A single forward slash ("/") is used to separate multiple SAP program identifiers in a portion mark or banner line
- A hyphen ("-") separates a SAP program and its compartments, if any
- A hyphen ("-") separates multiple compartments within a single SAP program
- A space separates a compartment from its sub-compartment(s), if any
- A space separates multiple sub-compartments within a single compartment

The *CAPCO Register and Manual* provides additional guidance on SAP Markings.

Select the image to zoom.

SAP Markings Sequence and Protocols

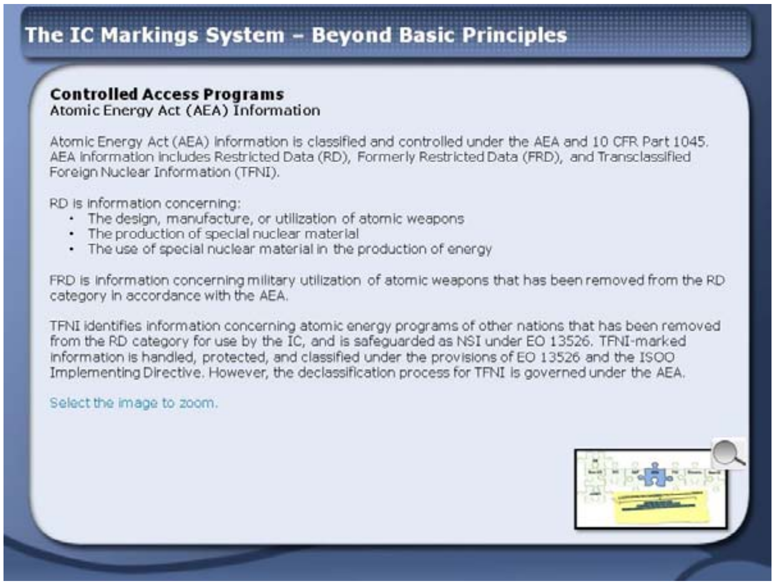
SAP Markings represent the fifth markings category in the *CAPCO Register* and *Manual*, and follow the classification level and any appropriate SCI Control System Markings in the portion mark and banner line sequence.

SAP Markings are required on all SAP material. All SAPs have SAP identifiers that represent the program's assigned nickname, codeword, or abbreviation. Multiple SAP program identifiers (nickname, codeword, or abbreviation) are ordered alpha-numerically and the following separators must be used when marking SAP material:

- A double forward slash ("//") precedes any value in this category
- The first value in the SAP category will be the SAP category indicator, either "SPECIAL ACCESS REQUIRED-" or "SAR-" (authorized abbreviation)
- A single forward slash ("/") is used to separate multiple SAP program identifiers in a portion mark or banner line
- A hyphen ("-") separates a SAP program and its compartments, if any
- A hyphen ("-") separates multiple compartments within a single SAP program
- A space separates a compartment from its sub-compartment(s), if any
- A space separates multiple sub-compartments within a single compartment

The *CAPCO Register and Manual* provides additional guidance on SAP Markings.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Special Access Program piece highlighted. An example banner line highlights //SAP with additional information: //Special Access Required-ABC or //SAR-ABC.)



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
Atomic Energy Act (AEA) Information

Atomic Energy Act (AEA) information is classified and controlled under the AEA and 10 CFR Part 1045. AEA information includes Restricted Data (RD), Formerly Restricted Data (FRD), and Transclassified Foreign Nuclear Information (TFNI).

RD is information concerning:

- The design, manufacture, or utilization of atomic weapons
- The production of special nuclear material
- The use of special nuclear material in the production of energy

FRD is information concerning military utilization of atomic weapons that has been removed from the RD category in accordance with the AEA.

TFNI identifies information concerning atomic energy programs of other nations that has been removed from the RD category for use by the IC, and is safeguarded as NSI under EO 13526. TFNI-marked information is handled, protected, and classified under the provisions of EO 13526 and the ISOO Implementing Directive. However, the declassification process for TFNI is governed under the AEA.

Select the image to zoom.

Atomic Energy Act (AEA) Information

Atomic Energy Act (AEA) information is classified and controlled under the AEA and 10 CFR Part 1045. AEA information includes Restricted Data (RD), Formerly Restricted Data (FRD), and Transclassified Foreign Nuclear Information (TFNI).

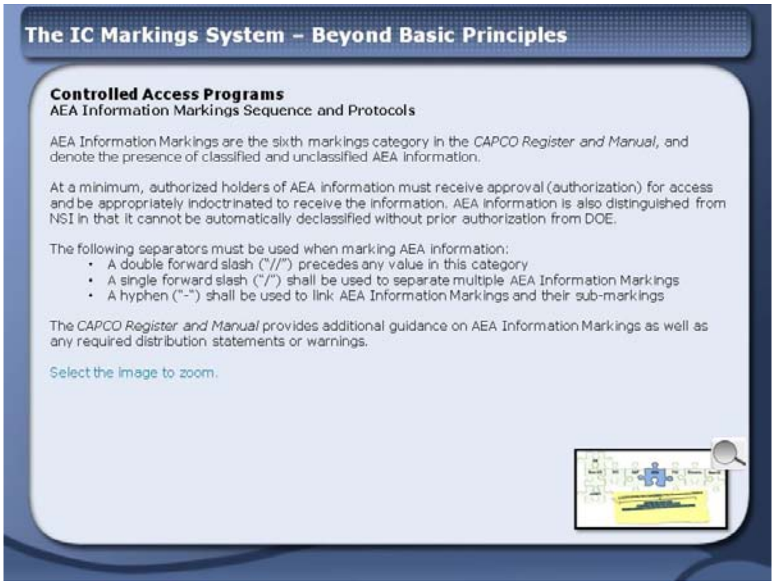
RD is information concerning:

- The design, manufacture, or utilization of atomic weapons
- The production of special nuclear material
- The use of special nuclear material in the production of energy

FRD is information concerning military utilization of atomic weapons that has been removed from the RD category in accordance with the AEA.

TFNI identifies information concerning atomic energy programs of other nations that has been removed from the RD category for use by the IC, and is safeguarded as NSI under EO 13526. TFNI-marked information is handled, protected, and classified under the provisions of EO 13526 and the ISOO Implementing Directive. However, the declassification process for TFNI is governed under the AEA.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the AEA piece highlighted. An example banner line highlights //AEA with additional information: RESTRICTED DATA (RD), FORMERLY RESTRICTED DATA (FRD), TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION (TFNI).)



The IC Markings System – Beyond Basic Principles

Controlled Access Programs
AEA Information Markings Sequence and Protocols

AEA Information Markings are the sixth markings category in the *CAPCO Register and Manual*, and denote the presence of classified and unclassified AEA information.

At a minimum, authorized holders of AEA information must receive approval (authorization) for access and be appropriately indoctrinated to receive the information. AEA information is also distinguished from NSI in that it cannot be automatically declassified without prior authorization from DOE.

The following separators must be used when marking AEA information:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") shall be used to separate multiple AEA Information Markings
- A hyphen ("-") shall be used to link AEA Information Markings and their sub-markings

The *CAPCO Register and Manual* provides additional guidance on AEA Information Markings as well as any required distribution statements or warnings.

Select the image to zoom.

AEA Information Markings Sequence and Protocols

AEA Information Markings are the sixth markings category in the *CAPCO Register and Manual*, and denote the presence of classified and unclassified AEA information.

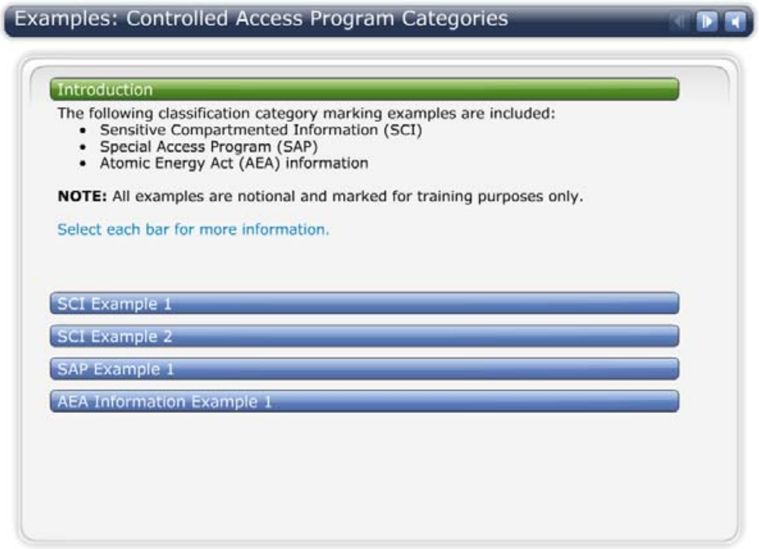
At a minimum, authorized holders of AEA information must receive approval (authorization) for access and be appropriately indoctrinated to receive the information. AEA information is also distinguished from NSI in that it cannot be automatically declassified without prior authorization from DOE.

The following separators must be used when marking AEA information:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") shall be used to separate multiple AEA Information Markings
- A hyphen ("-") shall be used to link AEA Information Markings and their sub-markings

The *CAPCO Register and Manual* provides additional guidance on AEA Information Markings as well as any required distribution statements or warnings.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Atomic Energy Act Information piece highlighted. An example banner line highlights AEA with additional information: RESTRICTED DATA (RD), FORMERLY RESTRICTED DATA (FRD), and TRANSCLASSIFIED FOREIGN NUCLEAR INFORMATION (TFNI).)



Examples: Controlled Access Program Categories

Introduction

The following classification category marking examples are included:

- Sensitive Compartmented Information (SCI)
- Special Access Program (SAP)
- Atomic Energy Act (AEA) information

NOTE: All examples are notional and marked for training purposes only.

Select each bar for more information.

SCI Example 1

SCI Example 2

SAP Example 1

AEA Information Example 1

Examples: Controlled Access Program Categories

Introduction

The following classification category marking examples are included:

- Sensitive Compartmented Information (SCI)
- Special Access Program (SAP)
- Atomic Energy Act (AEA) information

NOTE: All examples are notional and marked for training purposes only.

SCI Example 1

SECRET//TK//NOFORN

(S//TK//NF) This portion is classified SECRET (S), contains information from the TALENT KEYHOLE (TK) SCI control system, and is not releasable to foreign nationals (NOFORN (NF)).

(U) **NOTE:** The classification authority block is required on all US classified NSI. See the ISOO Implementing Directive and General Marking Guidance Section of the *CAPCO Register and Manual* for more information.

Classify By: __________
Derived From: _______
Declassify On: ________

SECRET//TK//NOFORN

SCI Example 2

TOP SECRET//SI-G//ORCON/NOFORN

(TS//SI-G//OC/NF) This portion is classified TOP SECRET (TS), contains information from the Special Intelligence (SI) SCI control system and the GAMMA (G) compartment, is Originator Controlled (ORCON (OC)), and not releasable to foreign nationals (NOFORN (NF)).

(U) **NOTE:** The classification authority block is required on all US classified NSI. See the ISOO Implementing Directive and General Marking Guidance Section of the *CAPCO Register and Manual* for more information.

Classify By: __________
Derived From: ______
Declassify On: _______

TOP SECRET//SI-G//ORCON/NOFORN

SAP Example 1

TOP SECRET//SAR-BP//NOFORN

(TS//SAR-BP//NF) This portion is classified TOP SECRET (TS), contains SPECIAL ACCESS REQUIRED-BUTTERED POPCORN (SAR-BP) information, and is not releasable to foreign nationals (NOFORN (NF)).

(U) **NOTE:** The classification authority block is required on all US classified NSI. See the ISOO Implementing Directive and General Marking Guidance Section of the *CAPCO Register and Manual* for more information.

Classify By: __________
Derived From: ______
Declassify On: _______

TOP SECRET//SAR-BP//NOFORN

AEA Information Example 1

SECRET//RESTRICTED DATA//NOFORN

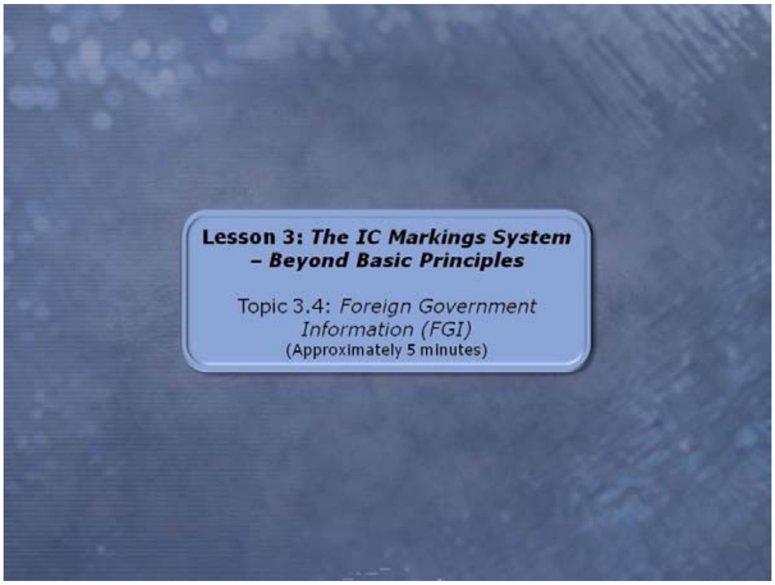
(S//RD//NF) This portion is classified SECRET (S), contains RESTRICTED DATA (RD), and is not releasable to foreign nationals (NOFORN (NF)).

(U) RESTRICTED DATA: This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure is subject to Administrative and Criminal Sanctions.

(U) **NOTE:** Automatic declassification of documents containing RD or FRD information is prohibited. If a document contains both AEA information and NSI, the "Declassify On" line of the classification authority block shall not include a declassification date or event, and shall instead be annotated with "Not Applicable (or N/A) to RD/FRD portions" and "See source list for NSI portions".

Classify By: ___________
Derived From: _______
Declassify On: ________

SECRET//RESTRICTED DATA//NOFORN



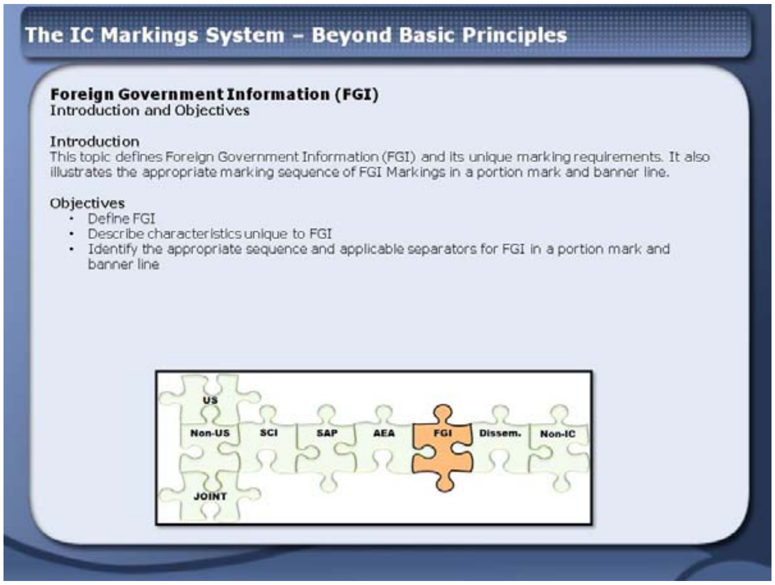
Lesson 3: *The IC Markings System – Beyond Basic Principles*

Topic 3.4: *Foreign Government Information (FGI)*
(Approximately 5 minutes)

Lesson 3: *The IC Marking System – Beyond Basic Principles*

Topic 3.4: *Foreign Government Information (FGI)*

(Approximately 5 minutes)



The IC Markings System – Beyond Basic Principles

Foreign Government Information (FGI)
Introduction and Objectives

Introduction
This topic defines Foreign Government Information (FGI) and its unique marking requirements. It also illustrates the appropriate marking sequence of FGI Markings in a portion mark and banner line.

Objectives
- Define FGI
- Describe characteristics unique to FGI
- Identify the appropriate sequence and applicable separators for FGI in a portion mark and banner line

Introduction and Objectives

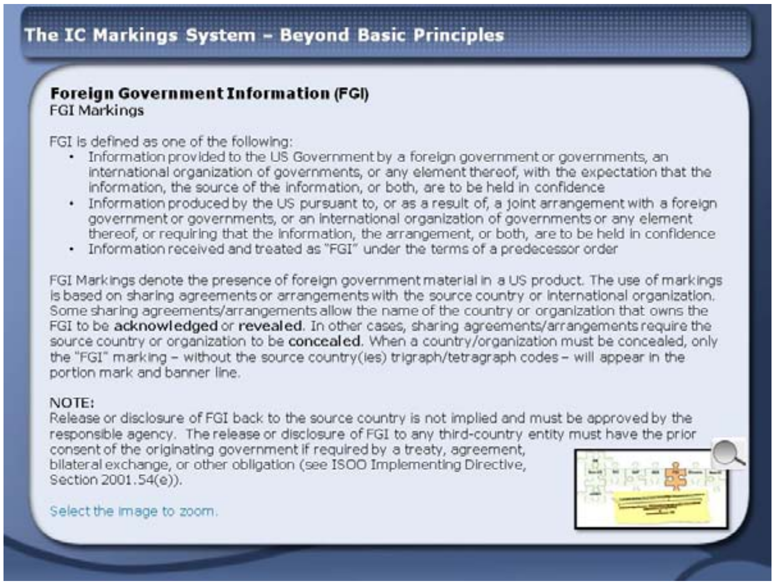
Introduction

This topic defines Foreign Government Information (FGI) and its unique marking requirements. It also illustrates the appropriate marking sequence of FGI Markings in a portion mark and banner line.

Objectives

- Define FGI
- Describe characteristics unique to FGI
- Identify the appropriate sequence and applicable separators for FGI in a portion mark and banner line

(Image alt: Puzzle pieces showing each of the nine categories of markings with the FGI piece highlighted.)



The IC Markings System – Beyond Basic Principles

Foreign Government Information (FGI)
FGI Markings

FGI is defined as one of the following:

- Information provided to the US Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence
- Information produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments or any element thereof, or requiring that the information, the arrangement, or both, are to be held in confidence
- Information received and treated as "FGI" under the terms of a predecessor order

FGI Markings denote the presence of foreign government material in a US product. The use of markings is based on sharing agreements or arrangements with the source country or international organization. Some sharing agreements/arrangements allow the name of the country or organization that owns the FGI to be **acknowledged** or **revealed**. In other cases, sharing agreements/arrangements require the source country or organization to be **concealed**. When a country/organization must be concealed, only the "FGI" marking – without the source country(ies) trigraph/tetragraph codes – will appear in the portion mark and banner line.

NOTE:
Release or disclosure of FGI back to the source country is not implied and must be approved by the responsible agency. The release or disclosure of FGI to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation (see ISOO Implementing Directive, Section 2001.54(e)).

Select the image to zoom.

FGI Markings

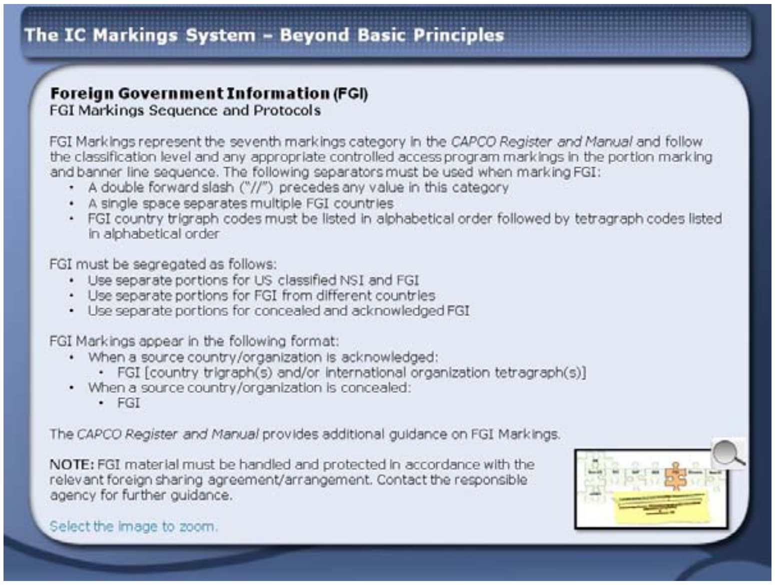
FGI is defined as one of the following:

- Information provided to the US Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence
- Information produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments or any element thereof, or requiring that the information, the arrangement, or both, are to be held in confidence
- Information received and treated as "FGI" under the terms of a predecessor order

FGI Markings denote the presence of foreign government material in a US product. The use of markings is based on sharing agreements or arrangements with the source country or international organization. Some sharing agreements/arrangements allow the name of the country or organization that owns the FGI to be **acknowledged** or **revealed**. In other cases, sharing agreements/arrangements require the source country or organization to be **concealed**. When a country/organization must be concealed, only the "FGI" marking – without the source country(ies) trigraph/tetragraph codes – will appear in the portion mark and banner line.

NOTES:
Release or disclosure of FGI back to the source country is not implied and must be approved by the responsible agency. The release or disclosure of FGI to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation (see ISOO Directive No. 1 2001.53(e)).

(Image alt: Puzzle pieces showing each of the nine categories of markings with the FGI piece highlighted. An example banner line highlights //FGI with additional information: Acknowledge Source – FGI [country trigraph and/or international organization tetragraph(s)] or Concealed Source - FGI.)



The IC Markings System – Beyond Basic Principles

Foreign Government Information (FGI)
FGI Markings Sequence and Protocols

FGI Markings represent the seventh markings category in the *CAPCO Register and Manual* and follow the classification level and any appropriate controlled access program markings in the portion marking and banner line sequence. The following separators must be used when marking FGI:

- A double forward slash ("//") precedes any value in this category
- A single space separates multiple FGI countries
- FGI country trigraph codes must be listed in alphabetical order followed by tetragraph codes listed in alphabetical order

FGI must be segregated as follows:

- Use separate portions for US classified NSI and FGI
- Use separate portions for FGI from different countries
- Use separate portions for concealed and acknowledged FGI

FGI Markings appear in the following format:

- When a source country/organization is acknowledged:
  - FGI [country trigraph(s) and/or international organization tetragraph(s)]
- When a source country/organization is concealed:
  - FGI

The *CAPCO Register and Manual* provides additional guidance on FGI Markings.

NOTE: FGI material must be handled and protected in accordance with the relevant foreign sharing agreement/arrangement. Contact the responsible agency for further guidance.

Select the image to zoom.

FGI Markings Sequence and Protocols

FGI Markings represent the seventh markings category in the *CAPCO Register and Manual* and follow the classification level and any appropriate controlled access program markings in the portion marking and banner line sequence. The following separators must be used when marking FGI:

- A double forward slash ("//") precedes any value in this category
- A single space separates multiple FGI countries
- FGI country trigraph codes must be listed in alphabetical order followed by tetragraph codes listed in alphabetical order

FGI must be segregated as follows:

- Use separate portions for US classified NSI and FGI
- Use separate portions for FGI from different countries
- Use separate portions for concealed and acknowledged FGI

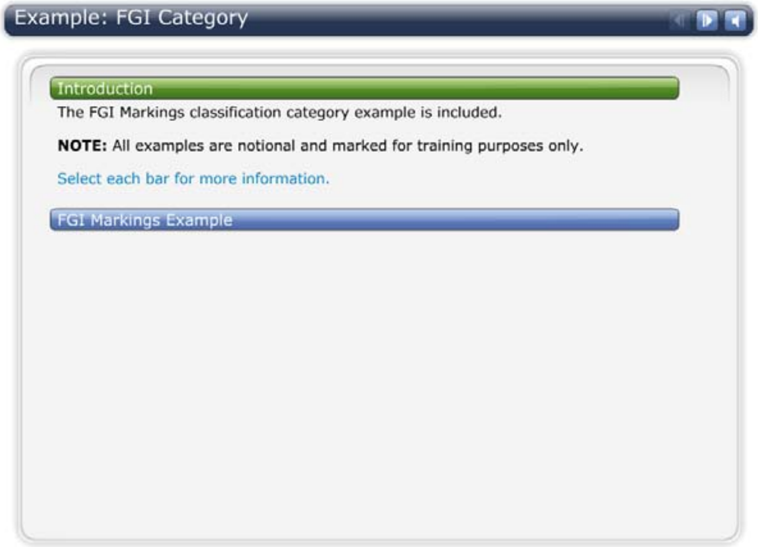
FGI Markings appear in the following format:

- When a source country/organization is acknowledged:
  - FGI [country trigraph(s) and/or international organization tetragraph(s)]
- When a source country/organization is concealed:
  - FGI

The *CAPCO Register and Manual* provides additional guidance on FGI Markings.

NOTE: FGI material must be handled and protected in accordance with the relevant foreign sharing agreement/arrangement. Contact the responsible agency for further guidance.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the FGI piece highlighted. An example banner line highlights //FGI with additional information: Acknowledge Source – FGI [country trigraph and/or international organization tetragraph(s)] or Concealed Source - FGI.)



Example: FGI Category

Introduction

The FGI Markings classification category example is included.

NOTE: All examples are notional and marked for training purposes only.

Select each bar for more information.

FGI Markings Example

Example: FGI Category

Introduction

The FGI Markings classification category example is included.

NOTE: All examples are notional and marked for training purposes only.

FGI Markings Example

TOP SECRET//FGI CAN DEU//REL TO USA, CAN, DEU

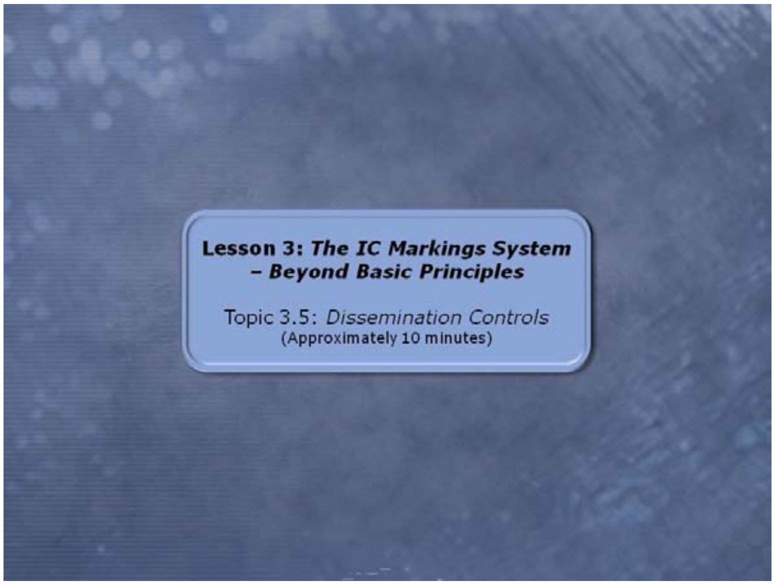
> (TS//REL TO USA, CAN, DEU) This portion is classified United States (USA) TOP SECRET (TS) and is authorized for release to (REL TO) Canada (CAN) and Germany (DEU).
>
> (//DEU S//REL TO USA, CAN, DEU) This portion is classified German (DEU) SECRET (S) within a US classified document, in which Germany has

authorized release (REL TO) back to Germany (DEU) and further release to (REL TO) United States (USA) and Canada (CAN).

(//CAN S//REL TO USA, CAN, DEU) This portion is classified Canada (CAN) SECRET (S) within a US classified document, in which Canada has authorized release (REL TO) back to Canada (CAN) and further release to (REL TO) United States (USA) and Germany (DEU).

(U) **NOTE:** Use the appropriate ISO 3166 trigraph country or international tetragraph code(s).
(U) **NOTE:** The classification authority block is required on all US classified NSI. See the ISOO Implementing Directive and General Markings Guidance Section of the *CAPCO Register and Manual* for more information.

TOP SECRET//FGI CAN DEU//REL TO USA, CAN, DEU



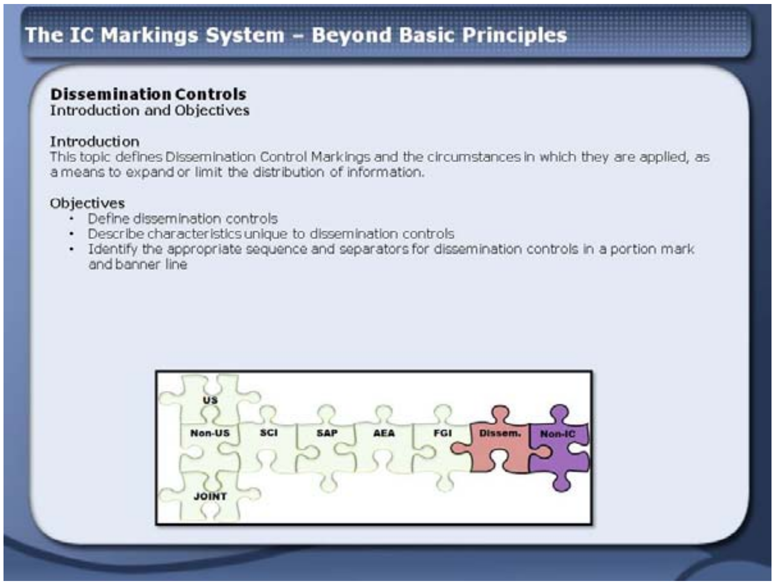
Lesson 3: ***The IC Markings System – Beyond Basic Principles***

Topic 3.5: *Dissemination Controls*
(Approximately 10 minutes)

Lesson 3: *The IC Marking System – Beyond Basic Principles*

Topic 3.5: *Dissemination Controls*

(Approximately 10 minutes)



The IC Markings System – Beyond Basic Principles

Dissemination Controls
Introduction and Objectives

Introduction
This topic defines Dissemination Control Markings and the circumstances in which they are applied, as a means to expand or limit the distribution of information.

Objectives
- Define dissemination controls
- Describe characteristics unique to dissemination controls
- Identify the appropriate sequence and separators for dissemination controls in a portion mark and banner line

Introduction and Objectives

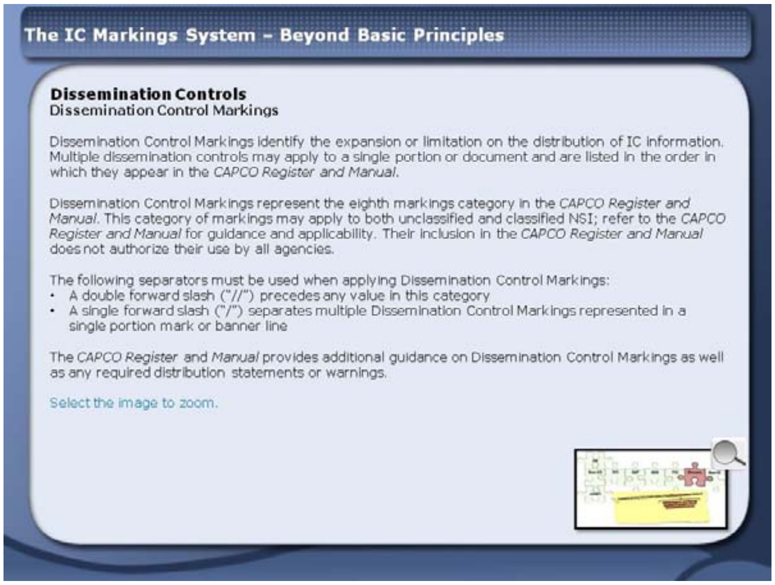
Introduction

This topic defines Dissemination Control Markings and the circumstances in which they are applied, as a means to expand or limit the distribution of information.

Objectives

- Define dissemination controls
- Describe characteristics unique to dissemination control
- Identify the appropriate sequence and separators for dissemination controls in a portion mark and banner line

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Dissem. and Non-IC pieces highlighted.)



The IC Markings System – Beyond Basic Principles

Dissemination Controls
Dissemination Control Markings

Dissemination Control Markings identify the expansion or limitation on the distribution of IC information. Multiple dissemination controls may apply to a single portion or document and are listed in the order in which they appear in the *CAPCO Register and Manual*.

Dissemination Control Markings represent the eighth markings category in the *CAPCO Register and Manual*. This category of markings may apply to both unclassified and classified NSI; refer to the *CAPCO Register and Manual* for guidance and applicability. Their inclusion in the *CAPCO Register and Manual* does not authorize their use by all agencies.

The following separators must be used when applying Dissemination Control Markings:
- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") separates multiple Dissemination Control Markings represented in a single portion mark or banner line

The *CAPCO Register* and *Manual* provides additional guidance on Dissemination Control Markings as well as any required distribution statements or warnings.

Select the image to zoom.

Dissemination Control Markings

Dissemination Control Markings identify the expansion or limitation on the distribution of IC information. Multiple dissemination controls may apply to a single portion or document and are listed in the order in which they appear in the *CAPCO Register and Manual*.

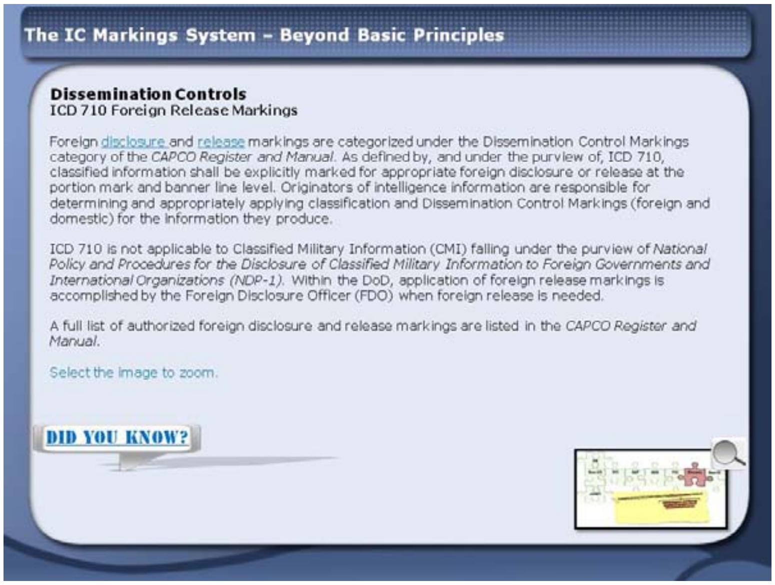
Dissemination Control Markings represent the eighth markings category in the *CAPCO Register and Manual*. This category of markings may apply to both unclassified and classified NSI; refer to the *CAPCO Register and Manual* for guidance and applicability. Their inclusion in the *CAPCO Register and Manual* does not authorize their use by all agencies.

The following separators must be used when applying Dissemination Control Markings:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") separates multiple Dissemination Control Markings represented in a single portion mark or banner line

The *CAPCO Register and Manual* provides additional guidance on Dissemination Control Markings as well as any required distribution statements or warnings.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Dissem. piece highlighted. An example banner line highlights //Dissemination with additional information: *CAPCO Register and Manual* provides a complete list of Dissemination Controls.)



The IC Markings System – Beyond Basic Principles

Dissemination Controls
ICD 710 Foreign Release Markings

Foreign disclosure and release markings are categorized under the Dissemination Control Markings category of the *CAPCO Register and Manual*. As defined by, and under the purview of, ICD 710, classified information shall be explicitly marked for appropriate foreign disclosure or release at the portion mark and banner line level. Originators of intelligence information are responsible for determining and appropriately applying classification and Dissemination Control Markings (foreign and domestic) for the information they produce.

ICD 710 is not applicable to Classified Military Information (CMI) falling under the purview of *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1)*. Within the DoD, application of foreign release markings is accomplished by the Foreign Disclosure Officer (FDO) when foreign release is needed.

A full list of authorized foreign disclosure and release markings are listed in the *CAPCO Register and Manual*.

Select the image to zoom.

ICD 710 Foreign Release Markings

Foreign disclosure and release markings are categorized under the Dissemination Control Markings category of the *CAPCO Register and Manual*. As defined by, and under the purview of, ICD 710, classified information shall be explicitly marked for appropriate foreign disclosure or release at the portion mark and banner line level. Originators of intelligence information are responsible for determining and appropriately applying classification and Dissemination Control Markings (foreign and domestic) for the information they produce.

ICD 710 is not applicable to Classified Military Information (CMI) falling under the purview of *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1)*. Within the DoD, application of foreign release markings is accomplished by the Foreign Disclosure Officer (FDO) when foreign release is needed.

A full list of authorized foreign disclosure and release markings are listed in the *CAPCO Register and Manual.*

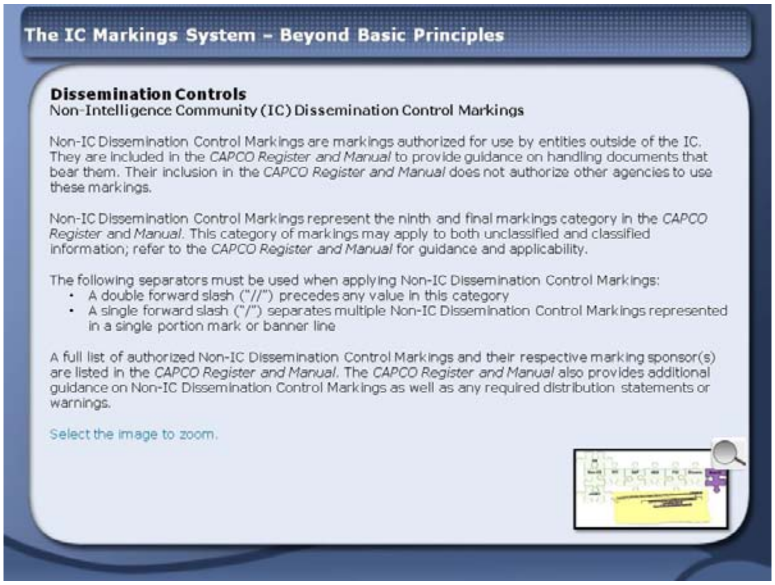
Pop Up: Disclosure
Under proper authority, the showing or revealing of classified NSI to a recipient, without providing the recipient with a physical copy for retention, regardless of medium.

Pop Up: Release
Under proper authority, providing the recipient of classified intelligence with a copy whether in writing or any other medium, of such information for retention.

Pop Up: Did You Know?

Some of the dissemination controls are restricted for use by certain agencies. They are included in the *CAPCO Register and Manual* to provide guidance on handing documents that bear them. Their including in the *Register and Manual* does not authorize their use by all agencies.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Dissem. piece highlighted. An example banner line highlights //Dissemination with additional information: *CAPCO Register and Manual* provides a complete list of Dissemination Controls.)



The IC Markings System – Beyond Basic Principles

Dissemination Controls
Non-Intelligence Community (IC) Dissemination Control Markings

Non-IC Dissemination Control Markings are markings authorized for use by entities outside of the IC. They are included in the *CAPCO Register and Manual* to provide guidance on handling documents that bear them. Their inclusion in the *CAPCO Register and Manual* does not authorize other agencies to use these markings.

Non-IC Dissemination Control Markings represent the ninth and final markings category in the *CAPCO Register* and *Manual*. This category of markings may apply to both unclassified and classified information; refer to the *CAPCO Register and Manual* for guidance and applicability.

The following separators must be used when applying Non-IC Dissemination Control Markings:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") separates multiple Non-IC Dissemination Control Markings represented in a single portion mark or banner line

A full list of authorized Non-IC Dissemination Control Markings and their respective marking sponsor(s) are listed in the *CAPCO Register and Manual*. The *CAPCO Register and Manual* also provides additional guidance on Non-IC Dissemination Control Markings as well as any required distribution statements or warnings.

Select the image to zoom.

Non-Intelligence Community (IC) Dissemination Control Markings

Non-IC Dissemination Control Markings are markings authorized for use by entities outside of the IC. They are included in the *CAPCO Register and Manual* to provide guidance on handling documents that bear them. Their inclusion in the *CAPCO Register and Manual* does not authorize other agencies to use these markings.

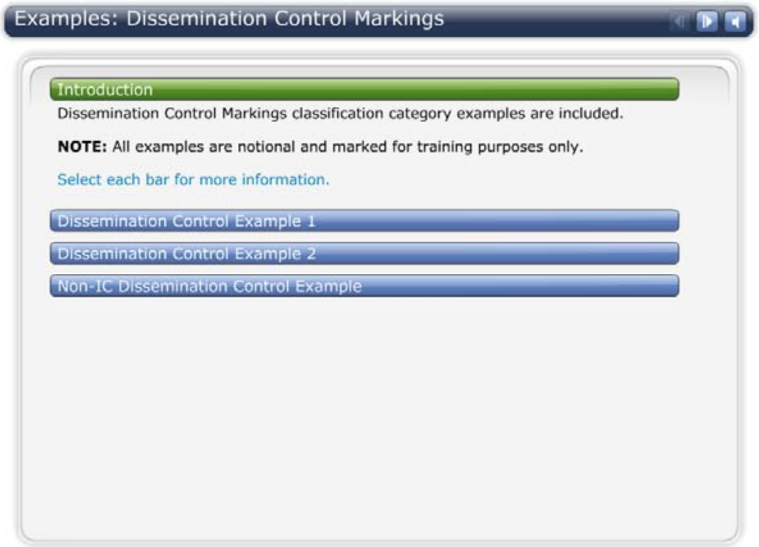
Non-IC Dissemination Control Markings represent the ninth and final markings category in the *CAPCO Register* and *Manual*. This category of markings may apply to both unclassified and classified information; refer to the *CAPCO Register and Manual* for guidance and applicability.

The following separators must be used when applying Non-IC Dissemination Control Markings:

- A double forward slash ("//") precedes any value in this category
- A single forward slash ("/") separates multiple Non-IC Dissemination Control Markings represented in a single portion mark or banner line

A full list of authorized Non-IC Dissemination Control Markings and their respective marking sponsor(s) are listed in the *CAPCO Register and Manual*. The *CAPCO Register and Manual also* provides additional guidance on Non-IC Dissemination Control Markings as well as any required distribution statements or warnings.

(Image alt: Puzzle pieces showing each of the nine categories of markings with the Non-IC piece highlighted. An example banner line highlights //NON-IC with additional information: *CAPCO Register and Manual* provides a complete list of Non-IC Dissemination Controls.)



Examples: Dissemination Control Markings

Introduction

Dissemination Control Markings classification category examples are included.

NOTE: All examples are notional and marked for training purposes only.

Select each bar for more information.

Dissemination Control Example 1
Dissemination Control Example 2
Non-IC Dissemination Control Example

Examples: Dissemination Control Markings

Introduction

Dissemination Control Markings classification category examples are included.

NOTE: All examples are notional and marked for training purposes only.

Dissemination Control Example 1

TOP SECRET//SI//PROPIN/REL TO USA, AUS, CAN, GBR

> (TS//SI//REL TO USA, FVEY) This portion is classified TOP SECRET (TS), contains information from the Special Intelligence (SI) SCI control system, in which the US has authorized release to (REL TO) United States (USA), Australia (AUS), Canada (CAN), United Kingdom (GBR), and New Zealand (NZL).

(S//SI//REL) This portion is classified SECRET (S), contains Special Intelligence (SI) controlled access program information, and is releasable to (REL TO) United States (USA), Australia (AUS), Canada (CAN) and United Kingdom (GBR). The abbreviation “REL” is permitted when the portion’s REL TO country/international organization list matches that of the banner line REL TO marking.

(S//PR//REL TO USA, FVEY) This portion is classified SECRET (S), contains proprietary information (PROPIN), in which the United States has authorized release to (REL TO) the FIVE EYES (FVEY) otherwise known as United States (USA), Australia (AUS), Canada (CAN), United Kingdom (GBR), and New Zealand (NZL).

(U) **NOTE:** The member countries of FVEY may be expanded for purposes of determining common country banner line roll-up. In this case, one portion provides a release dissemination control of “REL TO USA, AUS, CAN, GBR” and the other two are REL TO USA, FVEY (releasable to USA, AUS, CAN, GBR and NZL). The common countries between these portions are USA, AUS, CAN and GBR, so the banner line would roll-up to “REL TO USA, AUS, CAN, GBR”.

TOP SECRET//SI//PROPIN/REL TO USA, AUS, CAN, GBR

Dissemination Control Example 2

SECRET//NOFORN

(S//REL TO USA, DEU) This portion is classified SECRET (S) and is authorized for release to (REL TO) Germany (DEU).

(S//REL TO USA, JPN) This portion is classified SECRET (S) and is authorized for release to (REL TO) Japan (JPN).

(S//REL TO USA, CAN) This portion is classified SECRET (S) and is authorized for release to Canada (CAN).

(U) **NOTE:** Each portion is releasable, but none of the portions are releasable to the same foreign entity. Therefore NOFORN must roll-up to the banner line.

SECRET//NOFORN

Non-IC Dissemination Control Example

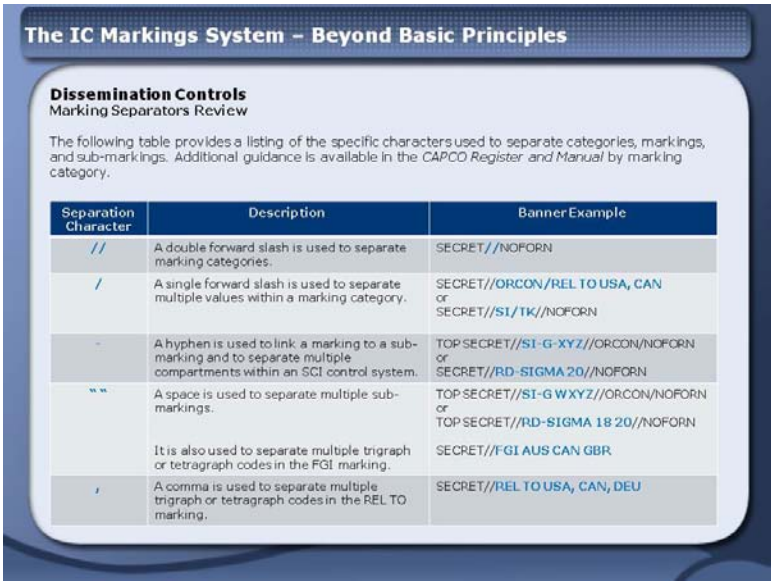
UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of (insert agency name here) and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without (insert agency name here) authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.

(U//LES) This portion is UNCLASSIFIED (U), and requires the dissemination control LAW ENFORCEMENT SENSITIVE (LES) to adequately protect the information.

(U) This portion is UNCLASSIFIED (U).

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



The IC Markings System – Beyond Basic Principles

Dissemination Controls
Marking Separators Review

The following table provides a listing of the specific characters used to separate categories, markings, and sub-markings. Additional guidance is available in the *CAPCO Register and Manual* by marking category.

Separation Character	Description	Banner Example
//	A double forward slash is used to separate marking categories.	SECRET//NOFORN
/	A single forward slash is used to separate multiple values within a marking category.	SECRET//ORCON/REL TO USA, CAN or SECRET//SI/TK//NOFORN
-	A hyphen is used to link a marking to a sub-marking and to separate multiple compartments within an SCI control system.	TOP SECRET//SI-G-XYZ//ORCON/NOFORN or SECRET//RD-SIGMA 20//NOFORN
" "	A space is used to separate multiple sub-markings. It is also used to separate multiple trigraph or tetragraph codes in the FGI marking.	TOP SECRET//SI-G WXYZ//ORCON/NOFORN or TOP SECRET//RD-SIGMA 18 20//NOFORN SECRET//FGI AUS CAN GBR
,	A comma is used to separate multiple trigraph or tetragraph codes in the REL TO marking.	SECRET//REL TO USA, CAN, DEU

Marking Separators Review

The following table provides a listing of the specific characters used to separate categories, markings, and sub-markings. Additional guidance is available in the *CAPCO Register* and *Manual* by marking category.

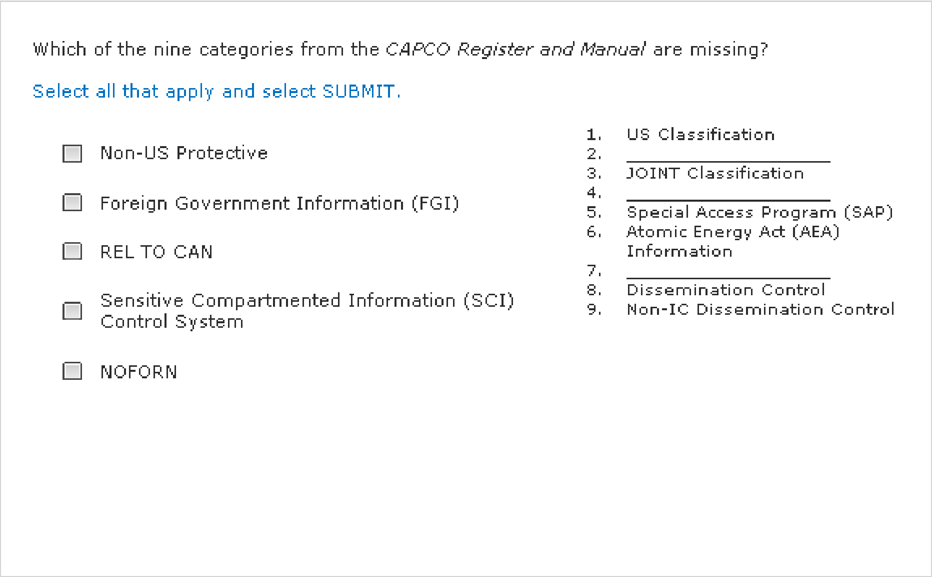
Separation Character	Description	Banner Example
//	A double forward slash is used to separate marking categories.	SECRET//NOFORN
/	A single forward slash is used to separate multiple values within a marking category.	SECRET//**ORCON/REL TO USA, CAN** or SECRET//**SI/TK**//NOFORN
-	A hyphen is used to link a marking to a sub-marking and to separate multiple compartments within an SCI control system.	TOP SECRET//**SI-G-XYZ**//ORCON/NOFORN or SECRET//**RD-SIGMA 20**//NOFORN
“ “	A space is used to separate multiple sub-markings.	TOP SECRET//**SI-G WXYZ**//ORCON/NOFORN or TOP SECRET//**RD-SIGMA 18 20**//NOFORN
	It is also used to separate multiple trigraph or tetragraph codes in the FGI marking	SECRET//**FGI AUS CAN GBR**
,	A comma is used to separate multiple trigraph or tetragraph codes in the REL TO marking.	SECRET//**REL TO USA, CAN, DEU**

Lesson 3 Knowledge Check

Introduction

The knowledge check consists of 13 questions.
(Approximately 25 minutes)

NOTE: All examples are notional and are marked for training purposes only.



Which of the nine categories from the *CAPCO Register and Manual* are missing?

Select all that apply and select SUBMIT.

□ Non-US Protective

□ Foreign Government Information (FGI)

□ REL TO CAN

□ Sensitive Compartmented Information (SCI) Control System

□ NOFORN

1. US Classification
2. ________
3. JOINT Classification
4. ________
5. Special Access Program (SAP)
6. Atomic Energy Act (AEA) Information
7. ________
8. Dissemination Control
9. Non-IC Dissemination Control

Topic 3.1

1 of 13: Which of the nine categories from the *CAPCO Register and Manual* are missing?

Fill in the missing Classification Categories with the Options below and continue reading for correct and incorrect feedback.

Classification Categories

1. US Classification
2. ________
3. JOINT Classification
4. ________
5. Special Access Program (SAP)
6. Atomic Energy Act (AEA) Information
7. ________
8. Dissemination Control
9. Non-IC Dissemination Control

Options:

- Sensitive Compartmented Information (SCI) Control System
- Non-US Protective
- REL TO CAN
- Foreign Government Information (FGI)
- NOFORN

The correct answers are:

- Non-US Protective
- Foreign Government Information (FGI)
- Sensitive Compartmented Information (SCI) Control System

Feedback when correct:
That's right! The missing categories of markings are:

- Non-US Protective
- Sensitive Compartmented Information (SCI) Control System
- Foreign Government Information (FGI)

REL TO CAN (Releasable to Canada) and NOFORN (Not Releasable to Foreign Nationals) are examples of Dissemination Control Markings.

Feedback when incorrect:
No, you did not select the correct responses.

The missing categories of markings are:

- Non-US Protective
- Sensitive Compartmented Information (SCI) Control System
- Foreign Government Information (FGI)

REL TO CAN (Releasable to Canada) and NOFORN (Not Releasable to Foreign Nationals) are examples of Dissemination Control Markings.

2 of 13: Place the marking categories in the prescribed sequence in accordance with the *CAPCO Register and Manual*. Remember this is how they would appear in a portion mark and banner line.

Place the Classification Categories in the proper order and continue reading for correct and incorrect feedback.

Classification Categories

- Atomic Energy Act (AEA) Information
- Dissemination Control
- Foreign Government Information (FGI)
- Non-IC Dissemination Control
- Sensitive Compartmented Information (SCI) Control System
- Special Access Program (SAP)
- US Classification, Non-US Protective, or JOINT Classification

The correct order is:

1. US Classification, Non-US Protective, or JOINT Classification
2. Sensitive Compartmented Information (SCI) Control System
3. Special Access Program (SAP)
4. Atomic Energy Act (AEA) Information
5. Foreign Government Information (FGI)
6. Dissemination Control
7. Non-IC Dissemination Control

Feedback when correct:

That's right! The order for the categories of markings is:

1. US Classification, Non-US Protective, or JOINT Classification
2. Sensitive Compartmented Information (SCI) Control System
3. Special Access Program (SAP)
4. Atomic Energy Act (AEA) Information
5. Foreign Government Information (FGI)
6. Dissemination Control
7. Non-IC Dissemination Control

Feedback when incorrect:

No, you did not select the correct order. The order for the categories of markings is:

1. US Classification, Non-US Protective, or JOINT Classification
2. Sensitive Compartmented Information (SCI) Control System
3. Special Access Program (SAP)
4. Atomic Energy Act (AEA) Information
5. Foreign Government Information (FGI)
6. Dissemination Control
7. Non-IC Dissemination Control

Topic 3.2

3 of 13: Match the first three classification categories to their definition.

Select the correct Classification Category for each Definition and continue reading for correct and incorrect feedback.

Definition	Classification Category
Markings that represent the classification level of US information and are required on all US classified NSI	• JOINT Classification • Non-US Protective • US Classification
Markings used on information received from a foreign government or international organization	• JOINT Classification • Non-US Protective • US Classification
Markings used on information which is owned or produced by more than one country and/or international organization	• JOINT Classification • Non-US Protective • US Classification

The correct answers are:

- US Classification: Markings that represent the classification level of US information and are required on all US classified NSI
- Non-US Protective: Markings used on information received from a foreign government or international organization
- JOINT Classification: Markings used on information which is owned or produced by more than one country and/or international organization

Feedback when correct:

That's right! The correct definitions are:

- US Classification Markings represent the classification level of US information and are required on all US classified NSI
- Non-US Protective Markings are used on information received from a foreign government or international organization
- JOINT Classification Markings are used on information which is owned or produced by more than one country and/or international organization

Feedback when incorrect:

You did not select the correct responses. The correct definitions are:

- US Classification Markings represent the classification level of US information and are required on all US classified NSI
- Non-US Protective Markings are used on information received from a foreign government or international organization
- JOINT Classification Markings are used on information which is owned or produced by more than one country and/or international organization

4 of 13: Which of the following are characteristics unique to the first three classification marking categories?

Select all that apply and continue reading for correct and incorrect feedback.

- The three classification categories (US Classification Markings, Non-US Protective Markings, and JOINT Classification Markings) are mutually exclusive; only one may be used in a marking sequence
- The classification category is always spelled out in the banner line
- JOINT classification markings always start with a double forward slash ("//") followed by "JOINT" and the appropriate trigraph country codes and/or international organization tetragraph code
- Non-US Protective Markings always start with a double forward slash ("//")

The correct answers are:

- The three classification categories (US Classification Markings, Non-US Protective Markings, and JOINT Classification Markings) are mutually exclusive; only one may be used in a marking sequence
- The classification category is always spelled out in the banner line
- JOINT classification markings always start with a double forward slash (“//”) followed by “JOINT” and the appropriate trigraph country codes and/or international organization tetragraph code
- Non-US Protective Markings always start with a double forward slash (“//”)

Feedback when correct:

That's right! All the statements apply:

- The three classification categories (US Classification Markings, Non-US Protective Markings, and JOINT Classification Markings) are mutually exclusive; only one may be used in a marking sequence
- The classification category is always spelled out in the banner line
- JOINT classification markings always start with a double forward slash ("//") followed by "JOINT" and the appropriate trigraph country codes and/or international organization tetragraph code
- Non-US Protective Markings always start with a double forward slash ("//")

Feedback when incorrect:

You did not select the correct responses. All the statements apply:

- The three classification categories (US Classification Markings, Non-US Protective Markings, and JOINT Classification Markings) are mutually exclusive; only one may be used in a marking sequence
- The classification category is always spelled out in the banner line
- JOINT classification markings always start with a double forward slash ("//") followed by "JOINT" and the appropriate trigraph country codes and/or international organization tetragraph code
- Non-US Protective Markings always start with a double forward slash ("//")

Topic 3.3
5 of 13: Match the three controlled access categories to the appropriate definition.

Select the correct Classification Category for each Definition and continue reading for correct and incorrect feedback.

Definition	Classification Category
Classified NSI concerning or derived from intelligence sources, methods, or analytical processes	• Atomic Energy Act (AEA) Information • Special Access Program (SAP) • Sensitive Compartmented Information (SCI) Control System
Classified NSI that requires extraordinary protection as allowed by EO 13526	• Atomic Energy Act (AEA) Information • Special Access Program (SAP) • Sensitive Compartmented Information (SCI) Control System
Information classified and controlled under the Atomic Energy Act and 10 CFR Part 1045, as well as EO 13526 (for TFNI); automatic declassification of this information is prohibited	• Atomic Energy Act (AEA) Information • Special Access Program (SAP) • Sensitive Compartmented Information (SCI) Control System

The correct answers are:

- Sensitive Compartmented Information (SCI) Control System: Classified NSI concerning or derived from intelligence sources, methods, or analytical processes
- Special Access Program (SAP): Classified NSI that requires extraordinary protection as allowed by EO 13526
- Atomic Energy Act (AEA) Information: Information classified and controlled under the Atomic Energy Act and 10 CFR Part 1045, as well as EO 13526 (for TFNI); automatic declassification of this information is prohibited

Feedback when correct:

That's right! The correct definitions are:

- Sensitive Compartmented Information (SCI) Control System is classified NSI concerning or derived from intelligence sources, methods, or analytical processes
- Special Access Program (SAP) information is classified NSI that requires extraordinary protection as allowed by EO 13526
- Atomic Energy Act (AEA) Information is classified and controlled under the Atomic Energy Act and 10 CFR Part 1045, as well as EO 13526 (for TFNI); automatic declassification of this information is prohibited

Feedback when incorrect:

You did not select the correct responses. The correct definitions are:

- Sensitive Compartmented Information (SCI) Control System is classified NSI concerning or derived from intelligence sources, methods, or analytical processes
- Special Access Program (SAP) information is classified NSI that requires extraordinary protection as allowed by EO 13526
- Atomic Energy Act (AEA) Information is classified and controlled under the Atomic Energy Act and 10 CFR Part 1045, as well as EO 13526 (for TFNI); automatic declassification of this information is prohibited

6 of 13: Identify the characteristics unique to controlled access programs (Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Atomic Energy Act (AEA)).

Select all that apply and continue reading for correct and incorrect feedback.

- SCI, SAP, and AEA controlled programs require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure
- AEA is classified and controlled under the AEA and 10 CFR Part 1045 and cannot be automatically declassified without prior authorization from Department of Energy (DOE)
- SCI, SAP, and AEA controlled programs do not require a "need-to-know" for access

The correct answers are:

- SCI, SAP, and AEA controlled programs require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure
- AEA is classified and controlled under the AEA and 10 CFR Part 1045 and cannot be automatically declassified without prior authorization from Department of Energy (DOE)

Feedback when correct:

That's right! The characteristics unique to controlled access programs (SCI, SAP, and AEA) include:

- SCI, SAP, and AEA controlled programs require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure
- AEA is classified and controlled under the AEA and 10 CFR Part 1045 and cannot be automatically declassified without prior authorization from Department of Energy (DOE)

SCI, SAP, and AEA controlled programs all require a formal "need-to-know" for access.

Feedback when incorrect:

You did not select the correct responses. The characteristics unique to controlled access programs (SCI, SAP, and AEA) include:

- SCI, SAP, and AEA controlled programs require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure
- AEA is classified and controlled under the AEA and 10 CFR Part 1045 and cannot be automatically declassified without prior authorization from Department of Energy (DOE)

SCI, SAP, and AEA controlled programs all require a formal "need-to-know" for access.

7 of 13: The banner line is partially completed. Using the text in the portion as clues, select and apply the appropriate controlled access markings to complete the existing banner.

Reference the Sample Document, place the Markings in proper sequence to complete the banner line, and continue reading for correct and incorrect feedback.

Sample Document:

TOP SECRET______________//ORCON//NOFORN

(S//TK//NF) This portion is classified SECRET (S), contains information from the TALENT KEYHOLE (TK) SCI control system, and is not releasable to foreign nationals (NOFORN (NF)).

(TS//SI-G//OC/NF) This portion is classified TOP SECRET (TS), contains information from the Special Intelligence (SI) SCI control system and the GAMMA (G) compartment, is Originator Controlled (ORCON (OC)), and not releasable to foreign nationals (NOFORN (NF)).

(TS//SAR-BP//NF) This portion is classified TOP SECRET (TS), contains SPECIAL ACCESS REQUIRED-BUTTERED POPCORN (SAR-BP) information, and is not releasable to foreign nationals (NOFORN (NF)).

(S//RD//NF) This portion is classified SECRET (S) and contains RESTRICTED DATA (RD).

(U) RESTRICTED DATA: This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure is subject to Administrative and Criminal Sanctions.

TOP SECRET______________//ORCON//NOFORN

Markings:

- //RD
- //SAR-BP
- //TK/SI-G

The correct sequence is:

1. //TK/SI-G
2. //SAR-BP
3. //RD

Feedback when correct:

That's right! The correct sequence is:

1. //TK/SI-G
2. //SAR-BP
3. //RD

The full banner line is: TOP SECRET**//TK/SI-G//SAR-BP//RD**//ORCON/NOFORN

Feedback when incorrect:

You did not select the correct responses. The correct sequence is:

1. //TK/SI-G
2. //SAR-BP
3. //RD

The full banner line is: TOP SECRET**//TK/SI-G//SAR-BP//RD**//ORCON/NOFORN

Topic 3.4
8 of 13: Which of the following statements define Foreign Government Information?

Select all that apply and continue reading for correct and incorrect feedback.

- Information provided to the US Government by a foreign government or governments, an international organization of governments with the expectation that the information, the source of the information, or both, are to be held in confidence
- Information produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments or requiring that the information, the arrangement, or both, are to be held in confidence
- Information received and treated as "FGI" under the terms of a predecessor order
- Information that contains US classified content in addition to the foreign government content

The correct answers are:

- Information provided to the US Government by a foreign government or governments, an international organization of governments with the expectation that the information, the source of the information, or both, are to be held in confidence
- Information produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments or requiring that the information, the arrangement, or both, are to be held in confidence
- Information received and treated as "FGI" under the terms of a predecessor order

Feedback when correct:

That's right! The correct responses are:

- Information provided to the US Government by a foreign government or governments, an international organization of governments with the expectation that the information, the source of the information, or both, are to be held in confidence
- Information produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments or requiring that the information, the arrangement, or both, are to be held in confidence
- Information received and treated as "FGI" under the terms of a predecessor order

Portions may only contain one country's information per portion unless, JOINT information is indicated. If there are multiple countries in separate portions, they are aggregated under the FGI Markings category in the banner line.

Feedback when incorrect:

You did not select the correct responses. The correct responses are:

- Information provided to the US Government by a foreign government or governments, an international organization of governments with the expectation that the information, the source of the information, or both, are to be held in confidence
- Information produced by the US pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments or requiring that the information, the arrangement, or both, are to be held in confidence
- Information received and treated as "FGI" under the terms of a predecessor order

Portions may only contain one country's information per portion unless, JOINT information is indicated. If there are multiple countries in separate portions, they are aggregated under the FGI Markings category in the banner line.

9 of 13: Which of the following are characteristics unique for Foreign Government Information (FGI)?

Select all that apply and continue reading for correct and incorrect feedback.

- FGI marked information must be segregated from US information
- A single forward slash ("/") separates multiple FGI countries represented in a banner line
- When a source country/organization is acknowledged, the markings appear as "FGI [country trigraph(s) and/or international organization tetragraph(s)]"
- When a source country/organization is concealed, the marking appears as "FGI"

The correct answers are

- FGI marked information must be segregated from US information
- When a source country/organization is acknowledged, the markings appear as "FGI [country trigraph(s) and/or international organization tetragraph(s)]"
- When a source country/organization is concealed, the marking appears as "FGI"

Feedback when correct:

That's right! The unique FGI characteristics are:

- FGI marked information must be segregated from US information
- When a source country/organization is acknowledged, the markings appear as "FGI [country trigraph(s) and/or international organization tetragraph(s)]"
- When a source country/organization is concealed, the marking appears as "FGI"

A double forward slash ("//") separates this value from the other classification category markings but this characteristic is not unique to the FGI category.

Feedback when incorrect:

You did not select the correct responses. The unique FGI characteristics are:

- FGI marked information must be segregated from US information
- When a source country/organization is acknowledged, the markings appear as "FGI [country trigraph(s) and/or international organization tetragraph(s)]"
- When a source country/organization is concealed, the marking appears as "FGI"

A double forward slash ("//") separates this value from the other classification category markings but this characteristic is not unique to the FGI category.

10 of 13: The banner line is partially completed. Using the text in the portion as clues, select and apply the appropriate Foreign Government Information (FGI) Markings to complete the existing banner.

Reference the Sample Document, place the Markings in proper sequence to complete the banner line, and continue reading for correct and incorrect feedback.

Sample Document:

TOP SECRET______________//REL TO USA, CAN, DEU

(TS//REL TO USA, CAN, DEU) This portion is classified United States (USA) TOP SECRET (TS) and is authorized for release to (REL TO) Canada (CAN) and Germany (DEU).

(//DEU S//REL TO USA, CAN, DEU) This portion is classified German (DEU) SECRET (S) within a US classified document, in which Germany has authorized release (REL TO) back to Germany (DEU) and further release to (REL TO) United States (USA) and Canada (CAN).

(//CAN S//REL TO USA, CAN, DEU) This portion is classified Canada (CAN) SECRET (S) within a US classified document, in which Canada has authorized release (REL TO) back to Canada (CAN) and further release to (REL TO) United States (USA) and Germany (DEU).

TOP SECRET______________//REL TO USA, CAN, DEU

Markings:

- CAN
- DEU
- //FGI

The correct sequence is:

1. //FGI
2. CAN
3. DEU

Feedback when correct:

That's right. The correct sequence is:

1. //FGI
2. CAN
3. DEU

The full banner line is:
TOP SECRET**//FGI CAN DEU**//REL TO USA, CAN, DEU

Feedback when incorrect:

You did not select the correct responses. The correct sequence is:

1. //FGI
2. CAN
3. DEU

The full banner line is:
TOP SECRET**//FGI CAN DEU**//REL TO USA, CAN, DEU

Topic 3.5

11 of 13: Dissemination Controls identify the expansion or limitation on the distribution of IC information. Multiple Dissemination Controls may apply to a single portion or document, and are listed in the order in which they appear in the *CAPCO Register and Manual*.

Select True or False and continue reading for correct and incorrect feedback.

- True
- False

The correct answer is “True.”

Feedback when correct:
That's right! Dissemination Controls identify the expansion or limitation on the distribution of IC information. Multiple Dissemination Controls may apply to a single portion or document, and are listed in the order in which they appear in the *CAPCO Register and Manual*.

Feedback when incorrect:
You did not select the correct response. The correct answer is “True.”

Dissemination Controls identify the expansion or limitation on the distribution of IC information. Multiple Dissemination Controls may apply to a single portion or document, and are listed in the order in which they appear in the *CAPCO Register and Manual*.

12 of 13: Which of the following are characteristics of Dissemination Controls?

Select all that apply and continue reading for correct and incorrect feedback.

- May apply to classified information
- May apply to unclassified information
- Appropriate foreign disclosure or release markings are required on classified information as defined by and under the purview of ICD 710

The correct answers are:

- May apply to classified information
- May apply to unclassified information
- Appropriate foreign disclosure or release markings are required on classified information as defined by and under the purview of ICD 710

Feedback when correct:
That's right! The correct responses include all of the options. This category of markings may apply to both unclassified and classified information. Dissemination Controls are required on classified information as defined by and under the purview of ICD 710.

Feedback when incorrect:
You did not select the correct responses. The correct responses include all of the options. This category of markings may apply to both unclassified and classified information. Dissemination Controls are required on classified information as defined by and under the purview of ICD 710.

13 of 13: The banner line is partially completed. Using the text in the portion as clues, select and apply the appropriate Dissemination Control Markings to complete the existing banner.

Reference the Sample Document, place the Markings in proper sequence to complete the banner line, and continue reading for correct and incorrect feedback.

Sample Document:

TOP SECRET//SI____________

(TS//SI//REL TO USA, FVEY) This portion is classified TOP SECRET (TS), contains information from the Special Intelligence (SI) SCI control system, in which the US has authorized release to (REL TO) United States (USA), Australia (AUS), Canada (CAN), United Kingdom (GBR), and New Zealand (NZL).

(S//SI//REL TO USA, AUS, CAN, GBR) This portion is classified SECRET (S), contains Special Intelligence (SI) controlled access program information, and is releasable to (REL TO) Australia (AUS), Canada (CAN), and United Kingdom (GBR).

(S//PR//REL TO USA, FVEY) This portion is classified SECRET (S), contains proprietary information (PROPIN), in which the United States has authorized release to (REL TO) the FIVE EYES (FVEY) otherwise known as United States (USA), Australia (AUS), Canada (CAN), United Kingdom (GBR), and New Zealand (NZL).

(S//REL TO USA, DEU) This portion is classified United States (USA) SECRET (S) and is authorized for release to (REL TO) Germany (DEU).

(S//REL TO USA, JPN) This portion is classified United States (USA) SECRET (S) and is authorized for release to (REL TO) Japan (JPN).

(S//REL TO USA, CAN) This portion is classified United States (USA) SECRET (S) and is authorized for release to Canada (CAN).

TOP SECRET//SI____________

Markings:

- //NOFORN/PROPIN

- //PROPIN/REL TO USA, AUS, CAN, GBR
- //REL TO USA, FVEY
- //REL TO USA, CAN, JPN

The correct answer is:

- //NOFORN/PROPIN

Feedback when correct:

That's right. The correct Dissemination Control Markings are:

- //NOFORN/PROPIN

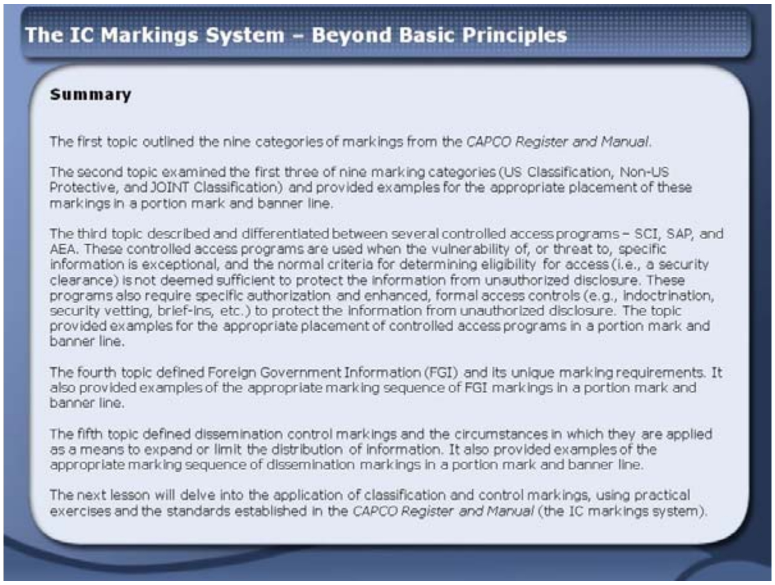
The full banner line is:
TOP SECRET//SI**//NOFORN/PROPIN**

Feedback when incorrect:

You did not select the correct response. The correct Dissemination Control Markings are:

- // NOFORN/PROPIN

The full banner line is:
TOP SECRET//SI**//NOFORN/PROPIN**



The IC Markings System – Beyond Basic Principles

Summary

The first topic outlined the nine categories of markings from the *CAPCO Register and Manual*.

The second topic examined the first three of nine marking categories (US Classification, Non-US Protective, and JOINT Classification) and provided examples for the appropriate placement of these markings in a portion mark and banner line.

The third topic described and differentiated between several controlled access programs – SCI, SAP, and AEA. These controlled access programs are used when the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access (i.e., a security clearance) is not deemed sufficient to protect the information from unauthorized disclosure. These programs also require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure. The topic provided examples for the appropriate placement of controlled access programs in a portion mark and banner line.

The fourth topic defined Foreign Government Information (FGI) and its unique marking requirements. It also provided examples of the appropriate marking sequence of FGI markings in a portion mark and banner line.

The fifth topic defined dissemination control markings and the circumstances in which they are applied as a means to expand or limit the distribution of information. It also provided examples of the appropriate marking sequence of dissemination markings in a portion mark and banner line.

The next lesson will delve into the application of classification and control markings, using practical exercises and the standards established in the *CAPCO Register and Manual* (the IC markings system).

Summary

The first topic outlined the nine categories of markings from the *CAPCO Register and Manual*.

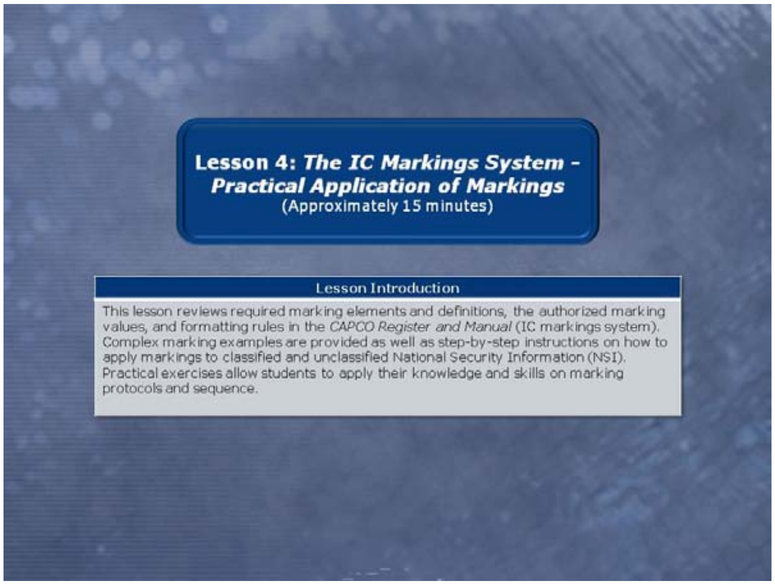
The second topic examined the first three of nine marking categories (US Classification, Non-US Protective, and JOINT Classification) and provided examples for the appropriate placement of these markings in a portion mark and banner line.

The third topic described and differentiated between several controlled access programs – SCI, SAP, and AEA. These controlled access programs are used when the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access (i.e., a security clearance) is not deemed sufficient to protect the information from unauthorized disclosure. These programs also require specific authorization and enhanced, formal access controls (e.g., indoctrination, security vetting, brief-ins, etc.) to protect the information from unauthorized disclosure. The topic provided examples for the appropriate placement of controlled access programs in a portion mark and banner line.

The fourth topic defined Foreign Government Information (FGI) and its unique marking requirements. It also provided examples of the appropriate marking sequence of FGI markings in a portion mark and banner line.

The fifth topic defined dissemination control markings and the circumstances in which they are applied as a means to expand or limit the distribution of information. It also provided examples of the appropriate marking sequence of dissemination markings in a portion mark and banner line.

The next lesson will delve into the application of classification and control markings, using practical exercises and the standards established in the *CAPCO Register and Manual* (the IC markings system).



Lesson 4: *The IC Markings System - Practical Application of Markings*
(Approximately 15 minutes)

Lesson Introduction

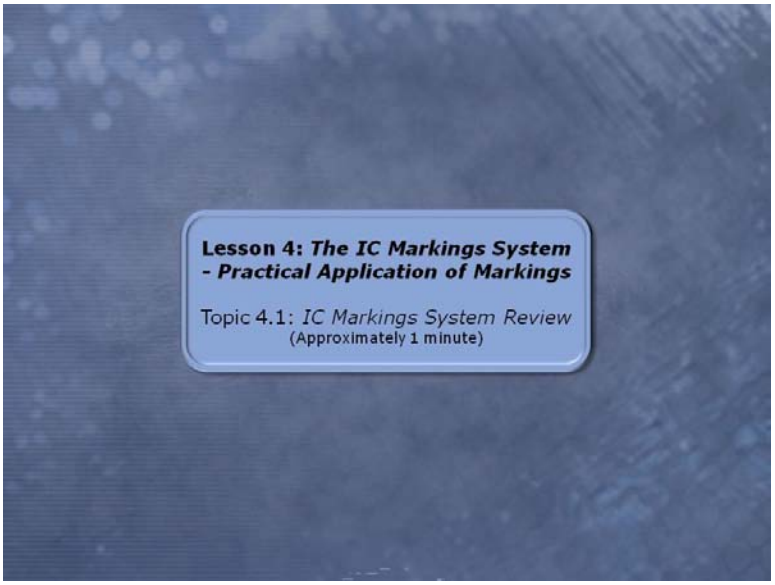
This lesson reviews required marking elements and definitions, the authorized marking values, and formatting rules in the *CAPCO Register and Manual* (IC markings system). Complex marking examples are provided as well as step-by-step instructions on how to apply markings to classified and unclassified National Security Information (NSI). Practical exercises allow students to apply their knowledge and skills on marking protocols and sequence.

Lesson 4: *The IC Markings System - Practical Application of Markings*

(Approximately 15 minutes)

Lesson Introduction

This lesson reviews required marking elements and definitions, the authorized marking values, and formatting rules in the *CAPCO Register and Manual* (IC markings system). Complex marking examples are provided as well as step-by-step instructions on how to apply markings to classified and unclassified National Security Information (NSI). Practical exercises allow students to apply their knowledge and skills on marking protocols and sequence.



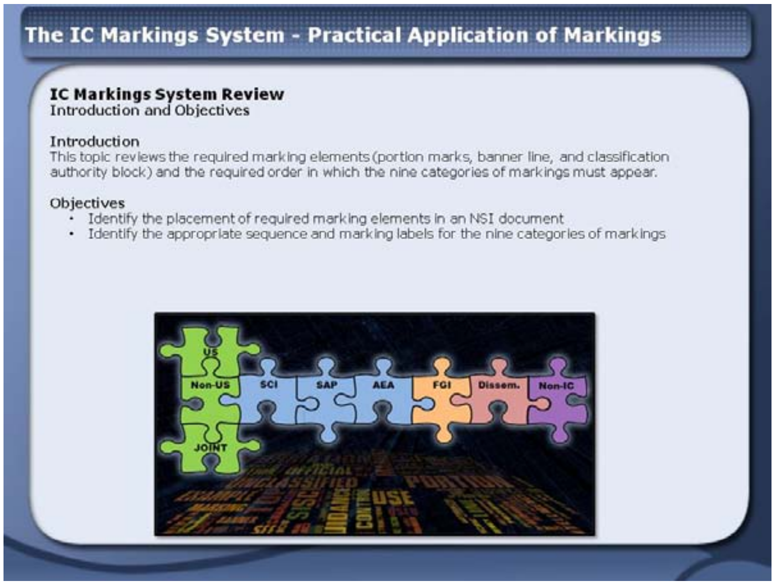
Lesson 4: *The IC Markings System - Practical Application of Markings*

Topic 4.1: *IC Markings System Review*
(Approximately 1 minute)

Lesson 4: *The IC Markings System - Practical Application of Markings*

Topic 4.1: *IC Markings System Review*

(Approximately 1 minute)



The IC Markings System - Practical Application of Markings

IC Markings System Review
Introduction and Objectives

Introduction
This topic reviews the required marking elements (portion marks, banner line, and classification authority block) and the required order in which the nine categories of markings must appear.

Objectives
- Identify the placement of required marking elements in an NSI document
- Identify the appropriate sequence and marking labels for the nine categories of markings

Introduction and Objectives

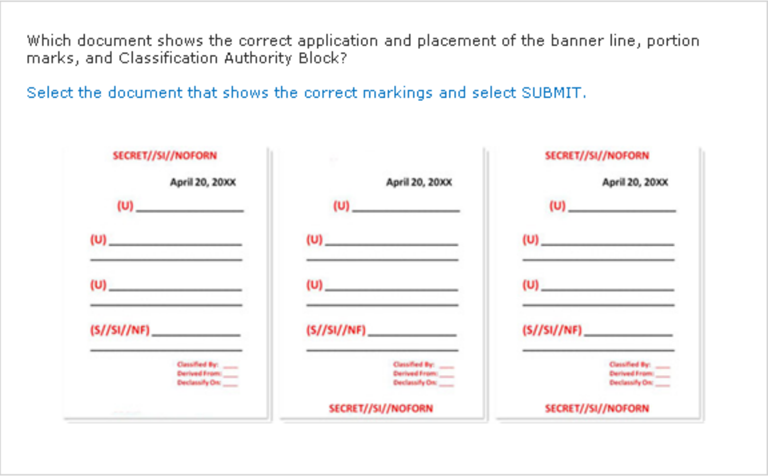
Introduction

This topic reviews the required marking elements (portion marks, banner line, and classification authority block) and the required order in which the nine categories of markings must appear.

Objectives

- Identify the placement of required marking elements in an NSI document
- Identify the appropriate sequence and marking labels for the nine categories of markings

(Image alt: Image of a puzzle with the nine categories of markings: US, Non-US, JOINT, SCI, SAP, AEA, FGI, Dissem., and Non-IC.)



Which document shows the correct application and placement of the banner line, portion marks, and Classification Authority Block?

Select the document that shows the correct markings and select SUBMIT.

Exercises: Marking Placement and Sequence

Introduction

The following exercises provide an opportunity to:

- Identify the placement of required marking elements in an NSI document
- Identify the appropriate sequence and marking labels for the nine categories of markings

(Approximately 5 minutes)

NOTE: All examples are notional and marked for training purposes only.

1 of 2: Which document shows the correct application and placement of the banner line, portion marks, and Classification Authority Block?

Select the document that shows the correct markings and continue reading for correct and incorrect feedback.

Document A:

SECRET//SI//NOFORN

April 20, 20XX

(U) ______________________________

(U) ______________________________
____

(U) ______________________________
____

(S//SI//NF) _____________________
____

Classified By: __________
Derived From: _________
Declassify On: _________

Document B:

April 20, 20XX

(U) ______________________________

(U) ______________________________
____

(U) ______________________________
____

(S//SI//NF) _____________________
____

Classified By: __________
Derived From: _________
Declassify On: _________

SECRET//SI//NOFORN

Document C:

SECRET//SI//NOFORN

April 20, 20XX

(U) ________________________________

(U) ________________________________
____

(U) ________________________________
____

(S//SI//NF) _________________________
____

Classified By: __________
Derived From: _________
Declassify On: __________

SECRET//SI//NOFORN

The correct answer is “Document C.”

Feedback when correct:
That's right. The banner line must be displayed at the top and bottom of the page, and must reflect the highest classification and most restrictive control markings in the document or individual page, in this case, **SECRET//SI//NOFORN**. The portion marks are correctly places at the beginning of the paragraphs and the Classification Authority Block is placed at the bottom right of the page.

Feedback when incorrect:
You did not provide the correct response. The correct response is “Document C.”

The banner line must be displayed at the top and bottom of the page, and must reflect the highest classification and most restrictive control markings in the document or individual page, in this case, **SECRET//SI//NOFORN.** The portion marks are correctly places at the beginning of the paragraphs and the Classification Authority Block is placed at the bottom right of the page.

2 of 2: Below is an example of a banner line and portion mark for each of the nine marking categories. Place the letter associated with each set of examples in the prescribed sequence in accordance with the *CAPCO Register and Manual*.

Place each letter in order and select SUBMIT.

Letter	Banner Line	Portion Mark
A.	//PROPIN	(//PR)
B.	//TALENT KEYHOLE	(//TK)
C.	TOP SECRET	(TS)
D.	//DEU SECRET	(//DEU S)
E.	//LAW ENFORCEMENT SENSITIVE	(//LES)
F.	//RESTRICTED DATA	(//RD)
G.	//FGI CAN	(//CAN TS)
H.	//JOINT SECRET CAN USA	(//JOINT S CAN USA)
I.	//SAR-BUTTERED POPCORN	(//SAR-BP)

The correct order is:

1. C
2. D
3. H
4. B
5. I
6. F
7. G
8. A
9. E

Feedback when correct:

That’s right! The order for the categories of marking is:

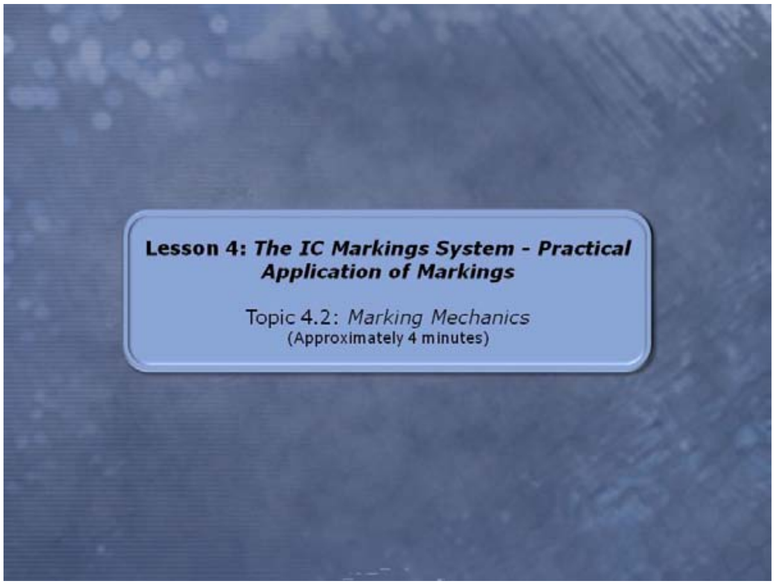
Letter	Banner Line	Portion Mark
C.	TOP SECRET	(TS)
D.	//DEU SECRET	(//DEU S)
H.	//JOINT SECRET CAN USA	(//JOINT S CAN USA)
B.	//TALENT KEYHOLE	(//TK)
I.	//SAR-BUTTERED POPCORN	(//SAR-BP)
F.	//RESTRICTED DATA	(//RD)
G.	//FGI CAN	(//CAN TS)
A.	//PROPIN	(//PR)
E.	//LAW ENFORCEMENT SENSITIVE	(//LES)

Feedback when incorrect:

You did not select the correct order.

The order for the categories of marking is:

Letter	Banner Line	Portion Mark
C.	TOP SECRET	(TS)
D.	//DEU SECRET	(//DEU S)
H.	//JOINT SECRET CAN USA	(//JOINT S CAN USA)
B.	//TALENT KEYHOLE	(//TK)
I.	//SAR-BUTTERED POPCORN	(//SAR-BP)
F.	//RESTRICTED DATA	(//RD)
G.	// FGI CAN	(//CAN TS)
A.	//PROPIN	(//PR)
E.	//LAW ENFORCEMENT SENSITIVE	(//LES)



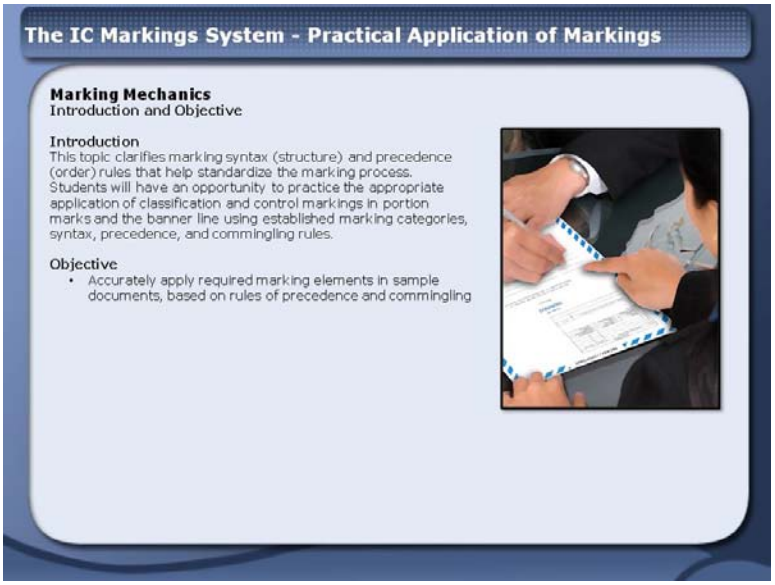
Lesson 4: *The IC Markings System - Practical Application of Markings*

Topic 4.2: *Marking Mechanics*
(Approximately 4 minutes)

Lesson 4: *The IC Markings System - Practical Application of Markings*

Topic 4.2: *Marking Mechanics*

(Approximately 4 minutes)



The IC Markings System - Practical Application of Markings

Marking Mechanics
Introduction and Objective

Introduction
This topic clarifies marking syntax (structure) and precedence (order) rules that help standardize the marking process. Students will have an opportunity to practice the appropriate application of classification and control markings in portion marks and the banner line using established marking categories, syntax, precedence, and commingling rules.

Objective
- Accurately apply required marking elements in sample documents, based on rules of precedence and commingling

Introduction and Objective

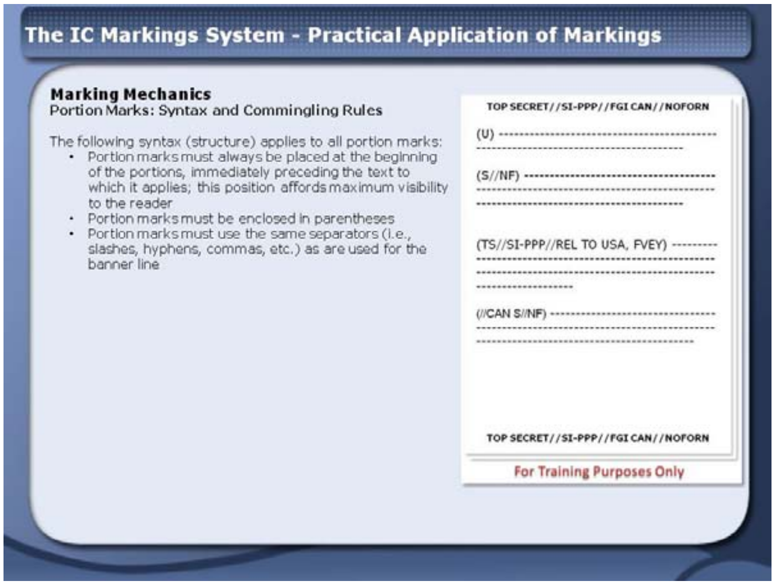
Introduction

This topic clarifies marking syntax (structure) and precedence (order) rules that help standardize the marking process. Students will have an opportunity to practice the appropriate application of classification and control markings in portion marks and the banner line using established marking categories, syntax, precedence, and commingling rules.

Objective

- Accurately apply required marking elements in sample documents, based on rules of precedence and commingling

(Image alt: A person accurately applying marking elements.)



The IC Markings System - Practical Application of Markings

Marking Mechanics
Portion Marks: Syntax and Commingling Rules

The following syntax (structure) applies to all portion marks:

- Portion marks must always be placed at the beginning of the portions, immediately preceding the text to which it applies; this position affords maximum visibility to the reader
- Portion marks must be enclosed in parentheses
- Portion marks must use the same separators (i.e., slashes, hyphens, commas, etc.) as are used for the banner line

```
TOP SECRET//SI-PPP//FGI CAN//NOFORN

(U) -------------------------------------
-----------------------------------

(S//NF) ---------------------------------
-----------------------------------------
-----------------------------------

(TS//SI-PPP//REL TO USA, FVEY) ---------
-----------------------------------------
-----------------------------------------
----------------

(//CAN S//NF) ---------------------------
-----------------------------------------
-------------------------------------

TOP SECRET//SI-PPP//FGI CAN//NOFORN
```

For Training Purposes Only

Portion Marks: Syntax and Commingling Rules

The following syntax (structure) applies to all portion marks:

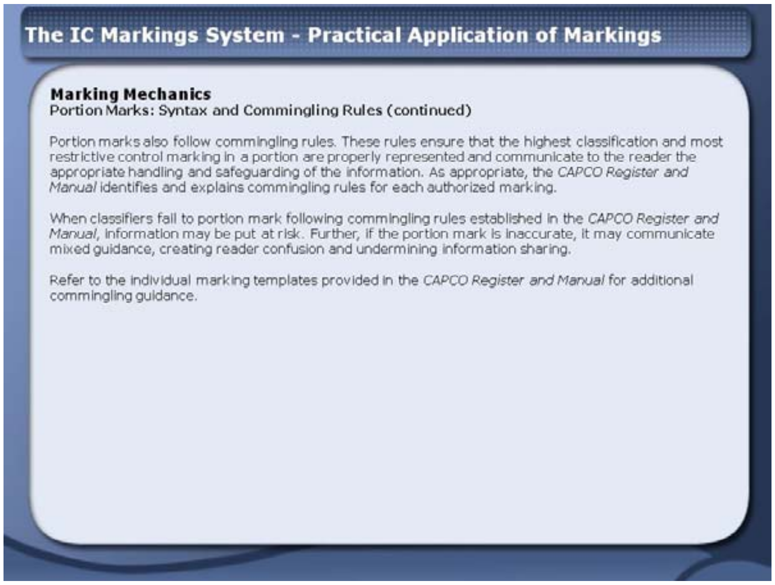
- Portion marks must always be placed at the beginning of the portions, immediately preceding the text to which it applies; this position affords maximum visibility to the reader
- Portion marks must be enclosed in parentheses
- Portion marks must use the same separators (i.e., slashes, hyphens, commas, etc.) as are used for the banner line

Example Document:

TOP SECRET//SI-PPP//FGI CAN//NOFORN

(U) ____.
(S//NF) ____
__________.
(TS//SI-PPP//REL TO USA, FVEY) ____________________________
____.
(//CAN S//NF) ____
____________________________.

TOP SECRET//SI-PPP//FGI CAN//NOFORN
For Training Purposes Only



The IC Markings System - Practical Application of Markings

Marking Mechanics
Portion Marks: Syntax and Commingling Rules (continued)

Portion marks also follow commingling rules. These rules ensure that the highest classification and most restrictive control marking in a portion are properly represented and communicate to the reader the appropriate handling and safeguarding of the information. As appropriate, the *CAPCO Register and Manual* identifies and explains commingling rules for each authorized marking.

When classifiers fail to portion mark following commingling rules established in the *CAPCO Register and Manual*, information may be put at risk. Further, if the portion mark is inaccurate, it may communicate mixed guidance, creating reader confusion and undermining information sharing.

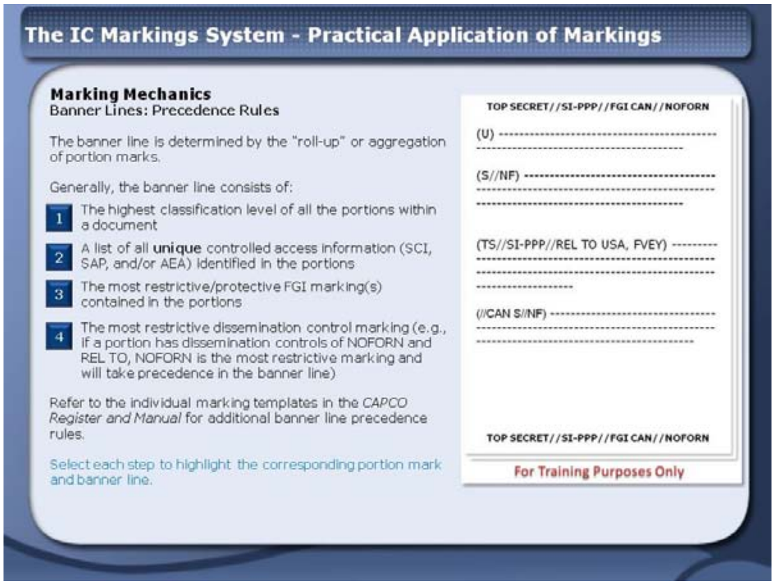
Refer to the individual marking templates provided in the *CAPCO Register and Manual* for additional commingling guidance.

Portion Marks: Syntax and Commingling Rules (continued)

Portion marks also follow commingling rules. These rules ensure that the highest classification and most restrictive control marking in a portion are properly represented and communicate to the reader the appropriate handling and safeguarding of the information. As appropriate, the *CAPCO Register and Manual* identifies and explains commingling rules for each authorized marking.

When classifiers fail to portion mark following commingling rules established in the *CAPCO Register and Manual*, information may be put at risk. Further, if the portion mark is inaccurate, it may communicate mixed guidance, creating reader confusion and undermining information sharing.

Refer to the individual marking templates provided in the *CAPCO Register and Manual* for additional commingling guidance.



The IC Markings System - Practical Application of Markings

Marking Mechanics
Banner Lines: Precedence Rules

The banner line is determined by the "roll-up" or aggregation of portion marks.

Generally, the banner line consists of:

1. The highest classification level of all the portions within a document
2. A list of all **unique** controlled access information (SCI, SAP, and/or AEA) identified in the portions
3. The most restrictive/protective FGI marking(s) contained in the portions
4. The most restrictive dissemination control marking (e.g., if a portion has dissemination controls of NOFORN and REL TO, NOFORN is the most restrictive marking and will take precedence in the banner line)

Refer to the individual marking templates in the *CAPCO Register and Manual* for additional banner line precedence rules.

Select each step to highlight the corresponding portion mark and banner line.

TOP SECRET//SI-PPP//FGI CAN//NOFORN

(U) --

(S//NF) --

(TS//SI-PPP//REL TO USA, FVEY) --

(//CAN S//NF) ---

TOP SECRET//SI-PPP//FGI CAN//NOFORN

For Training Purposes Only

Banner Lines: Precedence Rules

The banner line is determined by the "roll-up" or aggregation of portion marks.

Generally, the banner line consists of:

1. The highest classification level of all the portions within a document
2. A list of unique controlled access information (SCI, SAP, and/or AEA) identified in the portions
3. The most restrictive/protective FGI marking(s) contained in the portions
4. The most restrictive dissemination control marking (e.g., if a portion has dissemination controls of NOFORN and REL TO, NOFORN is the most restrictive marking and will take precedence in the banner line)

Refer to the individual marking templates in the *CAPCO Register and Manual* for additional banner line precedence rules.

Example Document:

TOP SECRET//SI-PPP//FGI CAN//NOFORN

(U) ____
____________________.

(S//NF) ____
____.

(TS//SI-PPP//REL TO USA, FVEY) ____________________________
____
__________.

(//CAN S//NF) ____
__________________________________ .

TOP SECRET//SI-PPP//FGI CAN//NOFORN

For Training Purposes Only

Popup Step 1:

(Image alt: (TS) portion mark and TOP SECRET banner lines highlighted.)

Popup Step 2:

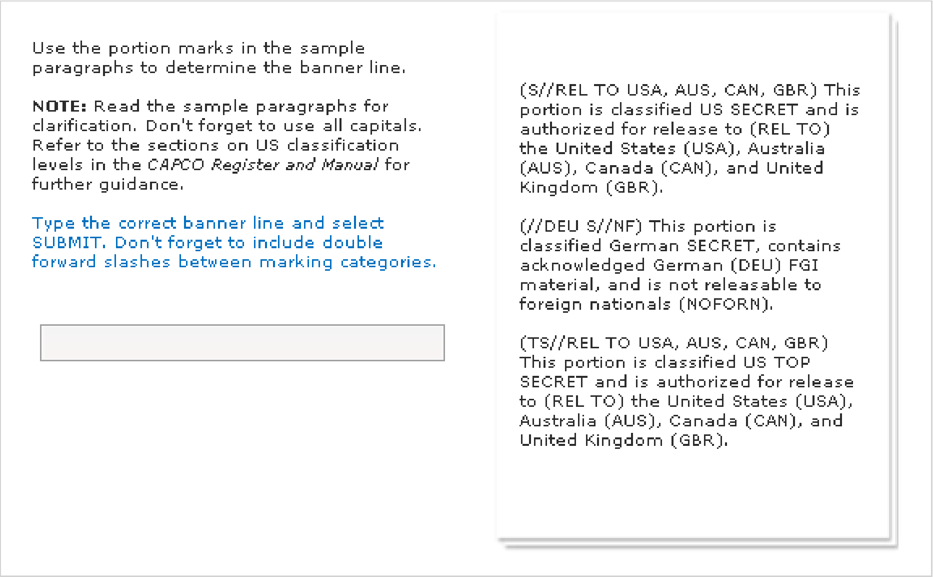
(Image alt: (//SI-PPP) portion mark and //SI-PPP banner lines highlighted.)

Popup Step 3:

(Image alt: (//CAN S) portion mark and //FGI CAN banner lines highlighted.)

Popup Step 4:

(Image alt: (//NF) portion marks and //NOFORN banner lines highlighted.)



Use the portion marks in the sample paragraphs to determine the banner line.

NOTE: Read the sample paragraphs for clarification. Don't forget to use all capitals. Refer to the sections on US classification levels in the *CAPCO Register and Manual* for further guidance.

Type the correct banner line and select SUBMIT. Don't forget to include double forward slashes between marking categories.

(S//REL TO USA, AUS, CAN, GBR) This portion is classified US SECRET and is authorized for release to (REL TO) the United States (USA), Australia (AUS), Canada (CAN), and United Kingdom (GBR).

(//DEU S//NF) This portion is classified German SECRET, contains acknowledged German (DEU) FGI material, and is not releasable to foreign nationals (NOFORN).

(TS//REL TO USA, AUS, CAN, GBR) This portion is classified US TOP SECRET and is authorized for release to (REL TO) the United States (USA), Australia (AUS), Canada (CAN), and United Kingdom (GBR).

Exercises: Applying Precedence Rules to the Banner Line

Introduction

The following exercises provide an opportunity to apply a banner using sample portion marks.

(Approximately 5 minutes)

NOTE: All examples are notional and marked for training purposes only.

1 of 2: Use the portion marks in the sample paragraphs to determine the banner line.

NOTE: Read the Sample Paragraphs for clarification. Don't forget to use all capitals. Refer to the sections on US classification levels in the *CAPCO Register and Manual* for further guidance.

Type the correct banner line and select SUBMIT. Don't forget to include double forward slashes between marking categories.

Sample Paragraphs:

(S//REL TO USA, AUS, CAN, GBR) This portion is classified US SECRET and is authorized for release to (REL TO) the United States (USA), Australia (AUS), Canada (CAN), and United Kingdom (GBR).

(//DEU S//NF) This portion is classified German SECRET, contains acknowledged German (DEU) FGI material, and is not releasable to foreign nationals (NOFORN).

(TS//REL TO USA, AUS, CAN, GBR) This portion is classified US TOP SECRET and is authorized for release to (REL TO) the United States (USA), Australia (AUS), Canada (CAN), and United Kingdom (GBR).

The correct answer is:
TOP SECRET//FGI DEU//NOFORN

Correctly Marked Document:

TOP SECRET//FGI DEU//NOFORN

(S//REL TO USA, AUS, CAN, GBR) This portion is classified US SECRET and is authorized for release to (REL TO) the United States (USA), Australia (AUS), Canada (CAN), and United Kingdom (GBR).

(//DEU S//NF) This portion is classified German SECRET, contains acknowledged German (DEU) FGI material, and is not releasable to foreign nationals (NOFORN).

(TS//REL TO USA, AUS, CAN, GBR) This portion is classified US TOP SECRET and is authorized for release to (REL TO) the United States (USA), Australia (AUS), Canada (CAN), and United Kingdom (GBR).

TOP SECRET//FGI DEU//NOFORN

Feedback when correct:
That's right.

- This document banner line appropriately reflects the highest classification level of the portion marks provided. Although two of the portions are classified SECRET, the highest classification of all the portions is TOP SECRET.
- The portion marks do not contain any SCI, SAP, and/or AEA Information Markings, therefore nothing is added to the banner line for those marking categories.
- The most restrictive FGI Markings contained in the portions must be represented in the banner line. In this case, acknowledged German (DEU) FGI material must be displayed in the banner line as "//FGI DEU".
- The most restrictive Dissemination Control Marking is NF and is displayed in the banner line as "//NOFORN".

Feedback when incorrect:
You did not provide the correct response:

- This document banner line appropriately reflects the highest classification level of the portion marks provided. Although two of the portions are classified SECRET, the highest classification of all the portions is TOP SECRET.

- The portion marks do not contain any SCI, SAP, and/or AEA Information Markings, therefore nothing is added to the banner line for those marking categories.
- The most restrictive FGI Markings contained in the portions must be represented in the banner line. In this case, acknowledged German (DEU) FGI material must be displayed in the banner line as "//FGI DEU".
- The most restrictive Dissemination Control Marking is NF and is displayed in the banner line as "//NOFORN".

2 of 2: Use the portion marks in the sample paragraphs to determine the banner line.

NOTE: Read the sample paragraphs for clarification and don't forget to use all capitals, use a double forward slash (//) to separate marking categories and a single forward slash (/) to separate multiple markings in the same category (or sub categories). Refer to the *CAPCO Register and Manual* for further guidance.

NOTE: Controlled access program markings may either be abbreviated or spelled out in the banner line if an authorized abbreviation is available.

Type the correct classification level for the banner line and select SUBMIT.

Sample Paragraphs:

> (TS//SAR-BP/SAR-SDA//NF) This portion is classified US TOP SECRET, contains BUTTERED POPCORN (BP) and SODA (SDA) Special Access Program information, and is not releasable to foreign nationals (NOFORN).
>
> (U//FOUO) This portion is UNCLASSIFIED and disseminated to US Government entities For Official Use Only (FOUO).
>
> (S//TK//RELIDO) This portion is classified as US SECRET, contains TALENT KEYHOLE (TK) and the originator of the information has determined it is releasable by an information disclosure official (RELIDO).

The correct answer is:
TOP SECRET//TK//SAR-BP/SAR-SDA//NOFORN

Correctly marked document:

TOP SECRET//TK//SAR-BP/SAR-SDA//NOFORN

> (TS//SAR-BP/SAR-SDA//NF) This portion is classified US TOP SECRET, contains BUTTERED POPCORN (BP) and SODA (SDA) Special Access Program information, and is not releasable to foreign nationals (NOFORN).
>
> (U//FOUO) This portion is UNCLASSIFIED and disseminated to US Government entities For Official Use Only (FOUO).
>
> (S//TK//RELIDO) This portion is classified as US SECRET, contains TALENT KEYHOLE (TK) and the originator of the information has determined it is releasable by an information disclosure official (RELIDO).

TOP SECRET//TK//SAR-BP/SAR-SDA//NOFORN

Feedback when correct:
That's right.

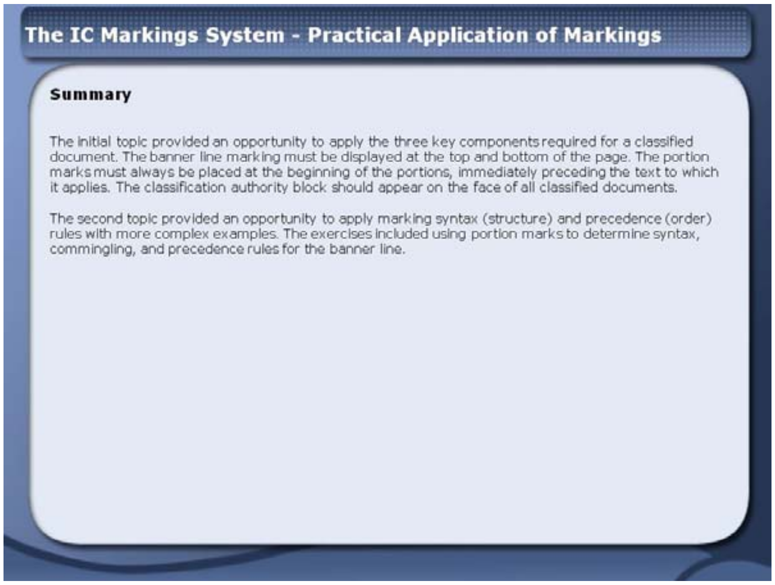
- The highest classification of all the portion marks is TOP SECRET.
- The controlled access program categories in the banner line are: //TK//SAR-BP/SAR-SDA. All unique controlled access program information - Sensitive Compartmented Information (SCI), Special Access Programs (SAP), and/or Atomic Energy Act (AEA) - used in document portion marks, must be displayed in the banner line.
  NOTE: (SAR-BP may also appear as SAR-BUTTERED POPCORN, SAR-SDA as SAR-SODA, TK as TALENT KEYHOLE, and RD as RESTRICTED DATA).
- None of the portion marks contain FGI, therefore nothing is added to the banner line for this marking category.
- The most restrictive Dissemination Control Marking is NF and is displayed in the banner line as “//NOFORN”.

NOTE: FOUO is a Dissemination Control for unclassified information, but is not conveyed in the banner line of a classified document because the classification level in the banner line adequately protects the controlled unclassified information in the U//FOUO portion.

Feedback when incorrect:
You did not provide the correct response.

- The highest classification of all the portion marks is TOP SECRET.
- The controlled access program categories in the banner line are: //TK//SAR-BP/SAR-SDA. All unique controlled access program information - Sensitive Compartmented Information (SCI), Special Access Programs (SAP), and/or Atomic Energy Act (AEA) - used in document portion marks, must be displayed in the banner line.
  NOTE: (SAR-BP may also appear as SAR-BUTTERED POPCORN, SAR-SDA as SAR-SODA, TK as TALENT KEYHOLE, and RD as RESTRICTED DATA).
- None of the portion marks contain FGI, therefore nothing is added to the banner line for this marking category.
- The most restrictive Dissemination Control Marking is NF and is displayed in the banner line as "//NOFORN".

NOTE: FOUO is a dissemination control for unclassified information, but is not conveyed in the banner line of a classified document because the classification level in the banner line adequately protects the controlled unclassified information in the U//FOUO portion.



The IC Markings System - Practical Application of Markings

Summary

The initial topic provided an opportunity to apply the three key components required for a classified document. The banner line marking must be displayed at the top and bottom of the page. The portion marks must always be placed at the beginning of the portions, immediately preceding the text to which it applies. The classification authority block should appear on the face of all classified documents.

The second topic provided an opportunity to apply marking syntax (structure) and precedence (order) rules with more complex examples. The exercises included using portion marks to determine syntax, commingling, and precedence rules for the banner line.

Summary

The initial topic provided an opportunity to apply the three key components required for a classified document. The banner line marking must be displayed at the top and bottom of the page. The portion marks must always be placed at the beginning of the portions, immediately preceding the text to which it applies. The classification authority block should appear on the face of all classified documents.

The second topic provided an opportunity to apply marking syntax (structure) and precedence (order) rules with more complex examples. The exercises included using portion marks to determine syntax, commingling, and precedence rules for the banner line.

Course Summary

Summary

The first lesson provided a brief history and background of classification management including authoritative policies and the foundation of the classification and control markings system. The lesson also emphasized the benefits of proper marking for optimizing information sharing and the protection of National Security Information (NSI).

The second lesson provided an overview of classification and control markings, including the required authorities, conditions for classification, the role of classification guidance documents, and other basic marking principles.

The third lesson identified and described the nine categories of classification and control markings. It also provided complex examples and step-by-step instructions on how to apply markings to NSI using proper marking protocols.

The fourth lesson reviewed required marking elements and definitions, the authorized marking values, and formatting rules in the *CAPCO Register and Manual* (IC markings system). Complex marking examples were provided, as well as step-by-step instructions on how to apply markings to classified and unclassified NSI. Practical exercises allowed students to apply their knowledge and skills on marking protocols and sequence.

Course Summary

The first lesson provided a brief history and background of classification management including authoritative policies and the foundation of the classification and control markings system. The lesson also emphasized the benefits of proper marking for optimizing information sharing and the protection of National Security Information (NSI).

The second lesson provided an overview of classification and control markings, including the required authorities, conditions for classification, the role of classification guidance documents, and other basic marking principles.

The third lesson identified and described the nine categories of classification and control markings. It also provided complex examples and step-by-step instructions on how to apply markings to NSI using proper marking protocols.

The fourth lesson reviewed required marking elements and definitions, the authorized marking values, and formatting rules in the *CAPCO Register and Manual* (IC markings system). Complex marking examples were provided, as well as step-by-step instructions on how to apply markings to classified and unclassified NSI. Practical exercises allowed students to apply their knowledge and skills on marking protocols and sequence.